NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER-SECURITY CURRICULA FOR BASIC USERS

by

Arthur L. Zepf IV

September 2013

Thesis Advisor: Zachary Peterson
Thesis Co-Advisor: Mark Gondree

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE CYBER-SECURITY CURRICULA FOR BASIC USERS	5. FUNDING NUMBERS
6. AUTHOR(S) Arthur L. Zepf IV	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release;distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

There have been only a small number of attempts at creating a cyber-security curriculum that can be used to teach children the concepts of cyber security and information assurance. There is a significant shortage of attempts at creating a computer-security curricula and cyber-security training for people who have only basic computer skills. Also, the integration of computer-security and information assurance principles into formal and accepted primary and secondary education is nearly non-existent. Our research has been aimed at evaluating the current computer-security curricula according to widely accepted educational standards. The objective is to (i) create a set of requirements to analyze the effectiveness of computer-security curricula, (ii) determine the best current disseminated cyber-security curriculum for children, (iii) and make recommendations for a cyber-security curriculum by utilizing the best traits of the surveyed programs. Literature includes studies on previously created computer-security curricula; and the most effective means of teaching children new concepts. Our research questions include: Is it important for a curriculum to be flexible enough to affect a variety of age groups? Is it important for a computer-security education to be interactive and motivational? Is it possible to teach difficult computer-security concepts in a way that children can understand?

14. SUBJECT TERMS Computer-security, cyber-security, education, curriculum, non-technical computer users, Internet safety.	15. NUMBER OF PAGES 93
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release;distribution is unlimited

CYBER-SECURITY CURRICULA FOR BASIC USERS

Arthur L. Zepf IV
Lieutenant, United States Navy
B.S., U.S. Naval Academy

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Arthur L. Zepf IV

Approved by: Zachary Peterson
Thesis Advisor

Mark Gondree
Thesis Co-Advisor

Peter Denning
Chair, Department of Computer Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There have been only a small number of attempts at creating a cyber-security curriculum that can be used to teach children the concepts of cyber security and information assurance. There is a significant shortage of attempts at creating a computer-security curricula and cyber-security training for people who have only basic computer skills. Also, the integration of computer-security and information assurance principles into formal and accepted primary and secondary education is nearly non-existent. Our research has been aimed at evaluating the current computer-security curricula according to widely accepted educational standards. The objective is to (i) create a set of requirements to analyze the effectiveness of computer-security curricula, (ii) determine the best current disseminated cyber-security curriculum for children, (iii) and make recommendations for a cyber-security curriculum by utilizing the best traits of the surveyed programs. Literature includes studies on previously created computer-security curricula; and the most effective means of teaching children new concepts. Our research questions include: Is it important for a curriculum to be flexible enough to affect a variety of age groups? Is it important for a computer-security education to be interactive and motivational? Is it possible to teach difficult computer-security concepts in a way that children can understand?

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

STEM	Science, Technology, Engineering, and Mathematics
NAEYC	National Association for the Education of Young Children
AMLE	Association for Middle Level Education
NSTA	National Science Teachers Association
NIST	National Institute for Standards and Technology
CNCI	Comprehensive National Cybersecurity Initiative
NICE	National Initiative for Cybersecurity Education
UNO	University of Nebraska at Omaha
USNA	United States Naval Academy
USMA	United States Military Academy
CERIAS	Center for Education and Research in Information Assurance and Security
CAE/IAE	Center of Academic Excellence in Information Assurance Education
NCWIT	National Council of Women and Information Technology
SLTT	State, Local, Tribal and Territorial
NCPC	National Crime Prevention Council
NCSA	National Cyber Security Alliance
ACMA	Australian Communications and Media Authority

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors for providing the motivation and inspiration for my work.

Thanks are due to all the members of my cohort at the Naval Postgraduate School. It is through your help and friendships that I gained so much experience and knowledge.

Most importantly, I would to thank my wife, Christina N. Zepf. Without your support, patience, understanding, and love, this work would never have been finished. I am very lucky to have you in my life. Charlotte, you gave me love, inspiration, and a much needed balance with my work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

During the last decade, the number of cyber-attacks and threats that Internet users are exposed to has exponentially grown. There is a significant need for everyday Internet users to understand and implement computer-security principles in online interactions. The Symantec Corporation suggests that almost 50% of cyber-attacks occur because basic users do not demonstrate simple security principles [1]. We believe that all basic Internet users should be exposed to a formal computer-security curriculum. Users who learn and practice cyber-security concepts do not only greatly reduce the chance that they are susceptible to cyber-attack, but they could also have a direct impact on the spread of attacks that permeate cyberspace. At the same time, organizations that require their employees to possess basic understanding of computer-security concepts could greatly reduce the negative effects of ignorant Internet actions [2]. Our research aims to survey the current landscape of computer-security curricula for non-technical users under the age of eighteen. We hope to determine the curriculum with the most effective means of teaching cyber-security concepts to children. We believe that teachers who utilize a computer-security curriculum that is accredited by a national academic organization can have a direct impact on this problem and will ensure their students' online safety and security.

The necessity for cyber-security training and education in public institutions and in private industry is directly linked to the growing threat landscape. In 1996, the National Institute for Standards and Technology (NIST) identified eight principles and fourteen practices that "provide a common ground for determining the security of an organization and build confidence when conducting multi-organizational business" [3] so that cyber-security and information assurance could be maintained by any organization. Later in 2000, NIST went on to expand this cyber-security education initiative to post-secondary and elementary students. This is illustrated in the introduction of the National Initiative for Cybersecurity Education-(NICE) framework, created after a cyber-security review completed by the Bush administration:

> The unfortunate reality is that relative to the magnitude of the threat, our ability and willingness to deal with threat have, on balance, changed for the worse, making many of the analyses, findings, and recommendations of these reports all the more relevant, timely, and applicable today [4].

As a result of this report, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI). In May of 2009, President Obama's Cyberspace Policy Review included an action item to "expand and train the workforce, including cyber-security expertise in the Federal government." One major outcome of President Obama's directive was the National Cybersecurity Workforce Framework, developed by NICE, that is to be used to develop nation-wide initiatives "focused on cybersecurity awareness, education, training, and professional development. Its goals are to encourage and help increase cyber-security awareness and competence across the nation and to build agile, highly skilled cyber-security workforce capable of responding to a dynamic and rapidly evolving array of threats" [4].

B. WHY TEACH CHILDREN?

Since there has been a drastic need for the growth of professionals with an understanding and experience with security principles, cyber-security education has shifted to the forefront of the federal cyber-warfare initiative. Some federal programs have emphasized the importance of beginning this training as early as possible in educational experiences. Many states have followed the lead of NICE and begun to create their own computer-security curricula that are to be integrated by elementary and secondary school teachers. Just as administrators have seen that foreign language acquisition has been shown to be especially effective at early stages in child development, so too has it been argued that young students should learn secure computer use early in their careers [5]. American children are increasingly using computers, mobile and other Internet-connected devices. It is imperative that they are exposed to cyber-security principles that will protect them and their environments from negative experiences. The Common Sense Media organization advocates a need for "Digital Literacy and Citizenship. This dynamic new world requires new comprehension and communication skills—as well as new codes of conduct—to ensure that these powerful

media and technologies are used responsibly and ethically" [6]. Establishing a baseline of computer-security knowledge may address demands of better security practices in this increasing threat landscape.

Computer-security education is fundamental to America's ability to stay protected and economically competitive and is important for a student's ability to safely navigate through an increasingly "online" world [4]. Cyber-security issues flood all aspects of everyday life. According to the CommonSenseMedia organization, "Kids and teens today are using the immense power of digital media to explore, connect, create, and learn in ways never before imagined. With this power, young people have extraordinary opportunities, and yet they face potential pitfalls…like cyberbullying, digital cheating, and safety and security concerns" [7]. The need to teach security principles to this age demographic is at an all-time high as of 2003, at which point 67% of children under the age of five and 75% of children ages 15 and older used a computer at home, statistics provided by the U.S. Department of Education [8]. Since then, it is believed these numbers have only increased, due in part to the changing use of computers in the educational process. In some states, schools provide computers to households that are unable to afford the purchase of a computer on their own. Through the assistance of computers, teachers are changing the dynamic of classrooms with a focus on technology. Teachers are using vastly different means of teaching their curricula to students. They have begun using an entirely different type of medium than teachers used a decade ago. Unfortunately, the importance of computer-security is not discussed in early educational environments. Rationale includes that there are too many technical complexities to teach in order to make a significant impact, or teaching computer-security concepts requires expensive resources. The very subject of cyber-security may be viewed as illicit, conjuring up negative connotations and various misconceptions. Generally, primary and secondary school teachers do not appear equipped with the tools to teach children about Internet safety and other computer security concepts because they don't have the knowledge themselves. A program that can teach children and teachers the basic tenets of cyber-security would set the standard for cyber-security curricula.

C. FINDING AN EFFECTIVE CURRICULUM

The goal of this research project is to survey the computer-security education landscape for curricula appropriate for young students. We desire to find a core set of modules covering those computer-security concepts that are pertinent to a wide audience, and may be integrated into curricula for STEM and non-STEM students. These cyber-security curricula should be intended to give students the foundation for future professional development in the cyber field.

Our study focuses on the examination of computer-security training modules for people with non-technical backgrounds early in their educational career, e.g., elementary school students. To-date, attempts to integrate computer-security and information assurance principles into primary education are very minimal. Our work attempts to determine the best designs, evaluate objectives of information assurance curriculums and delineate a set of requirements. After reviewing each independent curriculum, we make recommendations and consolidate the best features of these programs so that they may be utilized by teachers to create future lesson plans and assist in integrating into current curricula.

These training programs are tailored for primary and secondary school students, but a goal for future work is to be able to tailor these training modules for older audiences. The best curriculum would be malleable enough so it could be presented to undergraduate students and others with limited exposure to computer-security concepts.

II. RELATED WORK

Previous work supporting the development of computer-security curricula has been focused on either education in undergraduate and graduate settings or training professionals in a work environment. There are a large number of programs devoted to teaching IT professionals and members of the private sector about computer-security. There have been only a handful of attempts to target younger audiences. In this section we will present cyber-security programs that have been developed to teach children ranging in age from 1–18 years. We did not limit our research to one age group. Instead, we queried targeted programs that had an objective to teach people with no, or a very limited computer-security background. It is important to note that many of these programs do not date further back than 2009. We view this as evidence of the impact that President Bush's, and subsequently President Obama's, nation cyber-policy reviews have made.

Programs at the undergraduate level were low in number; we found only three that were specifically created to teach people with no computer or IT background. At the primary or secondary levels there were a much larger number, about nine different educational programs promoted teaching computer-security concepts and Internet safety. This included a couple of international programs, developed in New Zealand and Australia. During our search, we also found a number of U.S. government programs that ranged from federally mandated projects to grass-root initiatives. All of the programs had a similar goal: instructing cyber-security concepts from a minimal level of knowledge and increasing the level of complexity as the student becomes more acclimated with the subject.

A. COMPUTER-SECURITY TRAINING IN UNDERGRADUATE PROGRAMS

According to the 2011 U.S. Department of Education report, students entering their first year at a four-year institution have used computers in the past and some may be very proficient in their usage. About 81% of students in college use a computer at home and 84% use a computer at school [8]. Some undergraduate universities have recognized the need to offer freshmen-level courses focused on cyber-security and information

assurance. We review some notable examples of these curricula here, as their goals—i.e., communicating core lessons to broad audiences—are similar to our own.

1. University of Nebraska–Omaha

The University of Nebraska-Omaha (UNO) provides an introductory information assurance class for every freshman [9]. The course is intended to teach principles of computer-security and to provide "general awareness of computer-security issues among non-technical degree programs" to interested students throughout the campus. It was not intended to be a mandatory course for all students, but rather a supplement course to develop interest in IA. Since its creation in 2009, the course has attracted students from a broad-range of non-CS programs, including bioinformatics, music performance, psychology, public affairs and community service, and studio art.

UNO's IA class is comprised of lab exercises, discussion of current security articles, guest lectures by IA professionals and a research-oriented project at the end of the course. A course outline and learning objectives for IASC 1100 (Introduction to Information Security) is provided in the Appendix. UNO's initiative is notable in that it attempts to spread IA awareness earlier in academic careers than most academic institutions.

2. U.S. Naval Academy

Following President Obama's Cyberspace Policy Review, the U.S. Naval Academy (USNA) created a committee to review the possibility of creating a cyber-warfare course for all students, regardless of academic major or focus of study [10]. The result was a two-course sequence, the first part taught during the student's first year at the Academy, and the second course taught during their third year. Each course in the sequence is structured as two lecture hours and two lab hours per week. USNA struggled with how to deliver the course material to non-technical students when the course was commissioned to be a "technical-core course," a non-negotiable attribute as mandated by the USNA leadership [10]. The course syllabus targets developing students' understanding of the following: physical/virtual architecture of cyberspace, hands-on experience with cyberspace, DoD's five pillars of Information Assurance [11], and hands-on experience with some basic defensive and offensive practices in cyberspace. Each lab

requires the student to work at the command prompt. For example, in the "Wireless Network Assembly" Lab, students are required to enter commands that create a wireless 802.11 network to communicate with their classmates. This may be daunting to many students with no previous exposure to networks, but USNA has created labs with instructor insertion into steps, so that the pace of lab events are controlled and systematic [10].

Based on student feedback, USNA found that

> roughly 27 percent of the students felt they lacked some of the requisite knowledge/skills at the start of the course, but of those just 13 percent felt this deficiency was a problem. For each of the three main parts of the course, between 88–95 percent of the students indicated that they either had a much-better or somewhat-better understanding of the key issues involved [10].

In other words, as self-reported by the students after completion of the first year of instruction in 2010, "the course learning objectives were met by about 90 percent of the students" [10]. Below are the some examples of the class's learning objectives [10]:

a. USNA SI110 Course Learning Objectives

- **Describe** computers, operating systems, networks, the Internet and the Web with respect to: digital representations of information, their basic operation and associated tools, and the underlying architectures and protocols and how they are vulnerable to attack.
- Perform simple debugging and diagnosis: **analyze** and **explain** the output of programs and the results of shell commands and **infer** why certain actions are permitted or not in an information system.
- **Identify** and **describe** the desired properties of secure information systems and the tools that are used to provide them. **Explain** representative attacks and select appropriate prevention and mitigation measures.
- **Explain**, **differentiate**, and **perform** basic actions related to reconnaissance, attack, defense, and forensics of information systems.
- **Describe** cyber scenarios in which user decisions affect security, **identifying** the user's vs. the technology's responsibilities, and **explain** the consequences of potential user actions in terms of risk and the tradeoff between services and security.

b. USNA SI110 Course Themes

- Input, processing, and output of data at various levels of abstraction.
- The occurrence of and difficulty dealing with unexpected or improperly handled input to programs.
- The tension between offering services and providing security.
- Defense in depth; exploiting the access you have to gain the access you want (e.g., privilege escalation).
- Attack and Defense viewed in terms of violating/protecting the Pillars of IA.
- The user's role in security; technological limitations that attackers exploit to "trick" the user.

3. Other Examples

In 2003, the U.S. Military Academy (USMA) developed a course to teach information assurance concepts to students without technical backgrounds, called "The Policy and Strategy of Cyberwarfare (SS490) [12]. USMA's institutional goal focused on creating graduates with a firm understanding of IA to "securing our infrastructure" in the future. In 2003, a member of the USMA CS department described the intended learning objectives for non-technical students as "we just want them to have a realistic understanding of cyberspace and information security; an ability that we found lacking at the beginning of the course" [13]. These concepts were enforced through class discussions and basic hands-on laboratory experiences. A final capstone project was used to reemphasize important concepts. They were given a template for a real-world hot spot that gave the "students a fictitious but plausible goal for the U.S. and a mission to brief the National Command Authority on a plan to use cyber-warfare to support achieving the goal" [12]. The course focused primarily on government policy towards cyber warfare, and did not give students the opportunity to explore IA concepts or security principles in other contexts.

B. COMPUTER-SECURITY TRAINING IN ELEMENTARY SCHOOL PROGRAMS

The following programs were created to teach students about computer-security and Internet safety at K-12 levels. These programs have different usability and

procedures. Some require a proctor to teach the topics in a classroom or can be used at home individually or with a parent.

1. CERIAS

In 2002, Purdue University founded the Center for Education and Research in Information Assurance and Security (CERIAS). The center's focus has been to provide IA training and education opportunities, along with providing research to create IA training curricula for a variety of demographics. One target demographic for curricula development at CERIAS is children ages 5–18 [14]. One such lesson for this demographic is on the topic of safe instant messaging (see Figure 1). In this lesson, children are divided into three-person groups composed of a recorder, a sender and a decoy. The activity is to send messages between groups, and for each group to identify the decoy. The information hiding lesson's learning objectives state that "students will learn that people online may not be who they think they are" and, thus, that the information they see online may not be from people they trust.

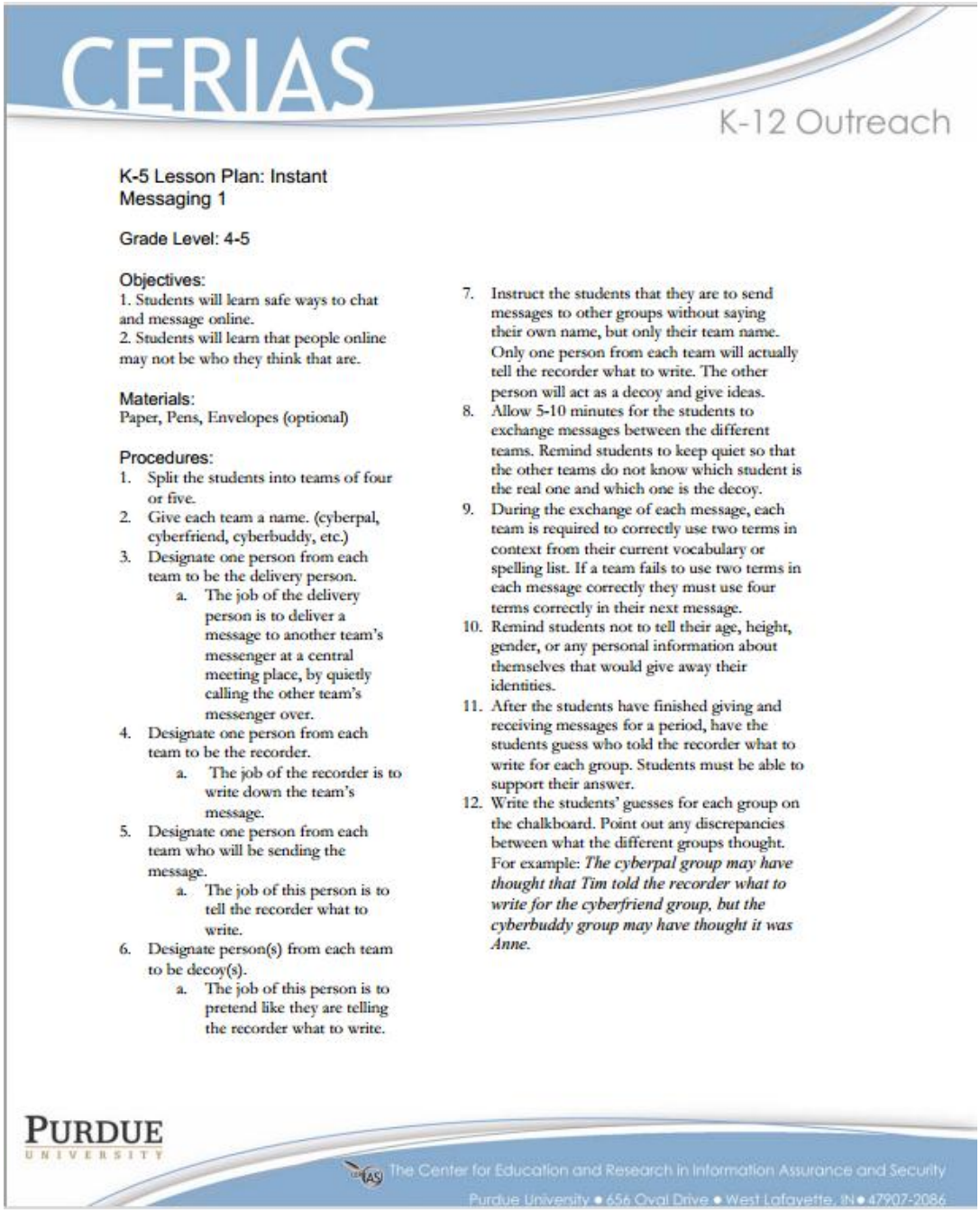
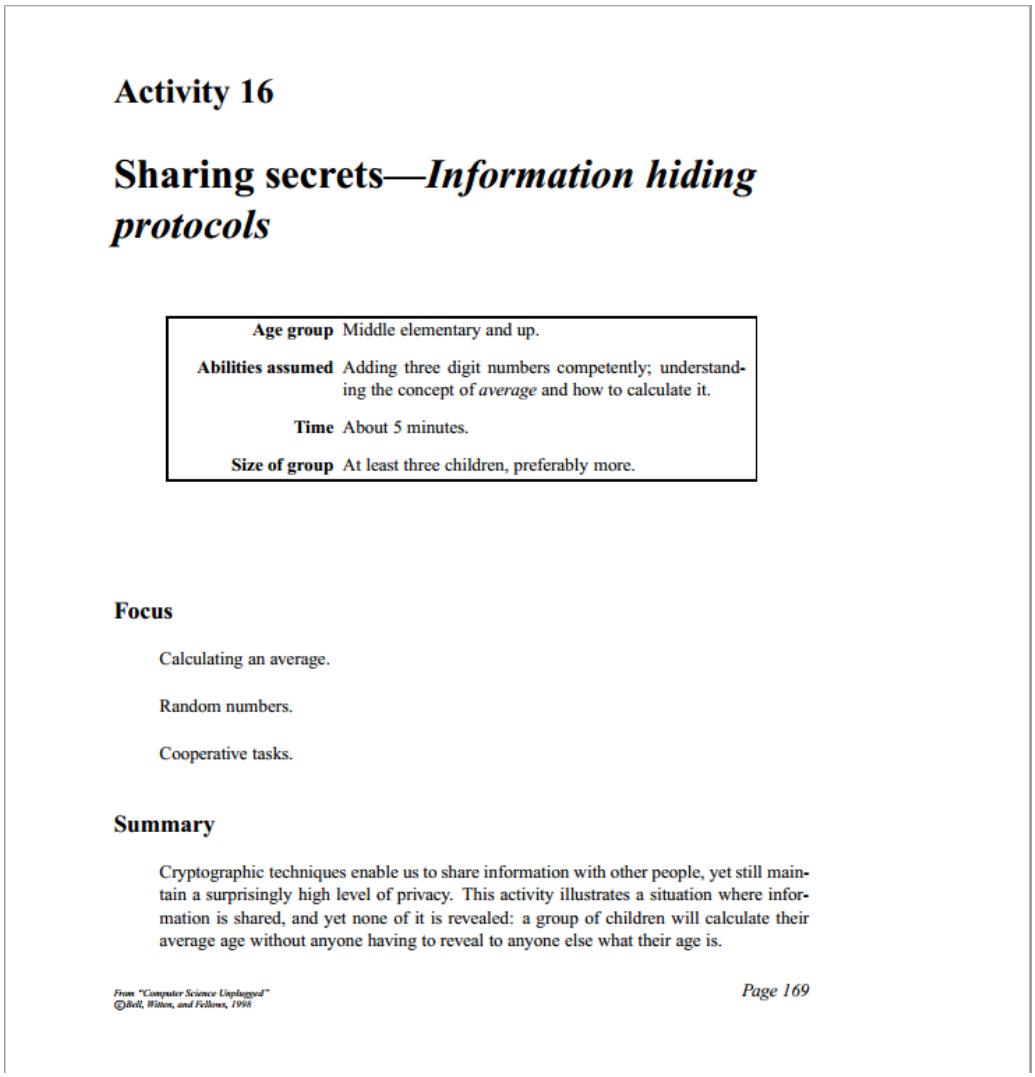


Figure 1. CERIAS Safe Instant Messaging Lesson Plan. From [14].

2. CS Unplugged

In 2009, Tim Bell founded "CS Unplugged," an online program that develops lessons teaching difficult computer science concepts without using a computer [15]. Designed by Bell and project contributors, these activities use cards, pen and pencil and other easily accessible materials, combined in activities modeled after children's games while illustrating some technical concept. These activities span numerous topics in computer science and, together, form a loose CS curriculum. Some of these activities cover security-relevant topics. For example, an activity on "information hiding" challenges students to try and determine the average age of a group of children, without any participants in the group revealing their age (see Figure 2). Each child adds their age to a secret, random number. This value is then passed to the next child who adds their age to the total, and this step is repeated for each child. The final sum is returned to first child, who subtracts the secret random number from the total and divides by the number of children to get the average. If two people choose to collaborate, some information can be determined; if everyone holds their observations secret, then no information is shared. CS Unplugged demonstrates, when the materials and procedures are kept relatively simple, that it is possible to devise lessons allowing widespread dissemination of a complex topic by educators that might not otherwise attempt to communicate those concepts. There are no studies completed that determine the effectiveness of these created lessons. However, there are organizations like the National Council of Women and Information (NCWIT), who recommend the CS Unplugged program based on its ease of use and portability to any classroom [16].



Activity 16

Sharing secrets—*Information hiding protocols*

Age group	Middle elementary and up.
Abilities assumed	Adding three digit numbers competently; understanding the concept of *average* and how to calculate it.
Time	About 5 minutes.
Size of group	At least three children, preferably more.

Focus

Calculating an average.

Random numbers.

Cooperative tasks.

Summary

Cryptographic techniques enable us to share information with other people, yet still maintain a surprisingly high level of privacy. This activity illustrates a situation where information is shared, and yet none of it is revealed: a group of children will calculate their average age without anyone having to reveal to anyone else what their age is.

Figure 2. CS Unplugged—Information Hiding Lesson Plan. From [15].

3. Cyber(smart:)

The Australian Communication and Media Authority (ACMA), an Australian government organization, created the program cyber(smart:). It is a "national cybersafety and cybersecurity education program as part of the Australian Government's commitment to cybersafety" [17]. The program is intended to "meet the needs of its target audiences of children, young people, parents, teachers and library staff." The program uses online resources to teach important cyber-security topics. Cyber(smart:) has created a number of online resources for children ages 1–7. One primary resource of cyber(smart:) is their focus on a storyline called "Hector's World." This narrative presents basic topics like

information hiding, cyber bullying, and computer-security. When utilizing this curriculum, teachers will use the provided narratives along with a variety of different stories or videos that discuss subjects like strong passwords, viruses and pop-ups. The website also includes lesson plans with activities like classroom discussions, Internet safety games, and promotes online safety through real-life narratives of people in the news who have been negatively affected by not practicing cyber-security. The program is very comprehensive and utilizes a variety of different media and teaching modes to communicate target topics. As all of these lessons are coupled with online resources, if a classroom does not have enough computers for each student then some resources cannot be utilized; the offline activities, used alone, may not be designed to present sufficient coverage for their target learning objectives.

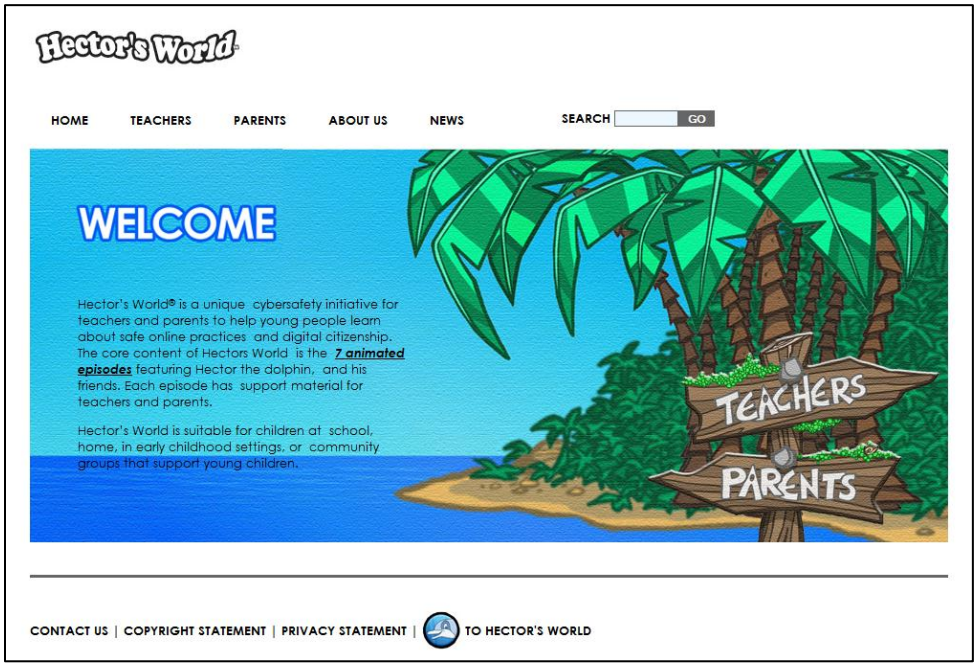
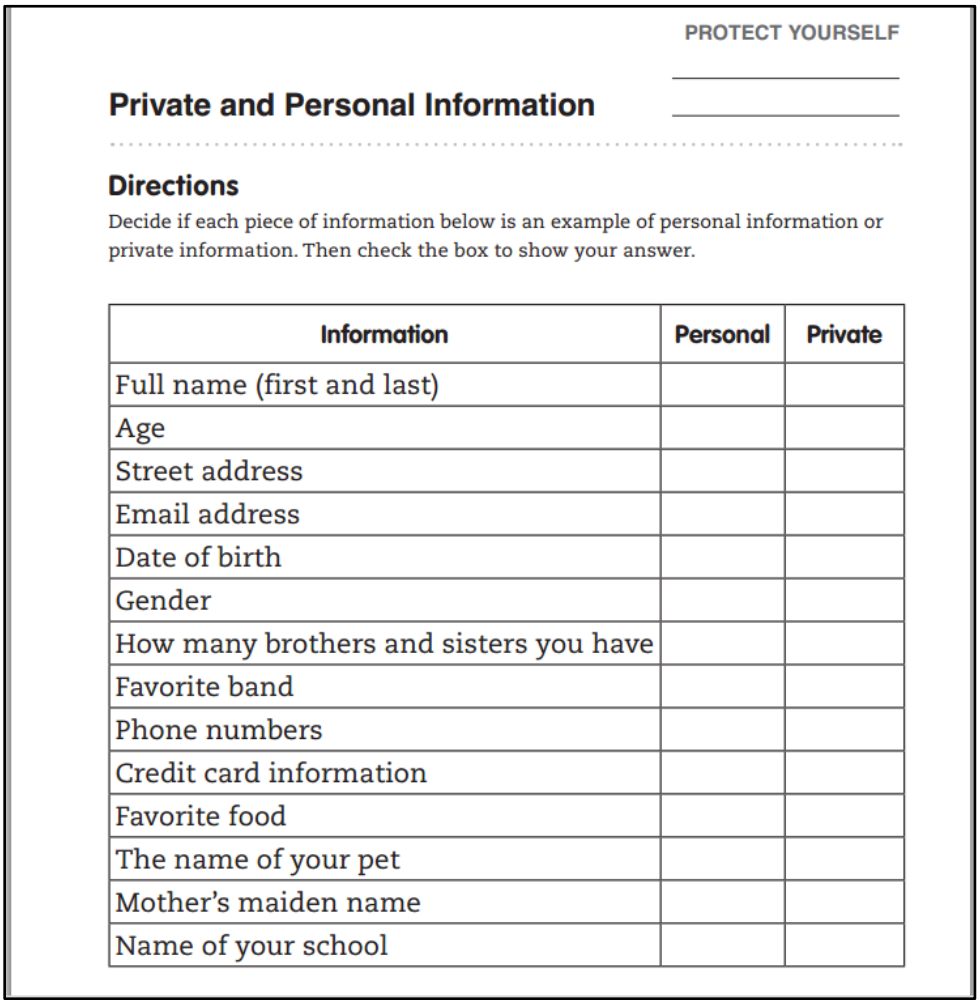


Figure 3. Hector's World—Narrative created to Teach Cyber-safety to children. From [17].

4. CyberSmart! Curriculum

The free CyberSmart! curriculum is a resource created by Common Sense Media [6]. This organization is "dedicated to improving the lives of kids and families by providing

the trustworthy information, education, and independent voice they need to thrive in a world of media and technology." They have created this curriculum that can be integrated into any school's current curriculum. Eighty lessons have been completed for the full K–12 curriculum. Supporting materials include student handouts, assessments, educational videos, family tip sheets, and professional development resources. The handouts and lesson plans are easy to follow, with suggested discussion topics. An important feature of each lesson is that most of the lessons may be completed by being connected to the Internet or with only basic classroom materials needed, i.e., pen, paper, blackboard, etc.



PROTECT YOURSELF

Private and Personal Information

Directions

Decide if each piece of information below is an example of personal information or private information. Then check the box to show your answer.

Information	Personal	Private
Full name (first and last)		
Age		
Street address		
Email address		
Date of birth		
Gender		
How many brothers and sisters you have		
Favorite band		
Phone numbers		
Credit card information		
Favorite food		
The name of your pet		
Mother's maiden name		
Name of your school		

Figure 4. CommonSenseMedia Grade 3–5 Worksheet—Information Hiding. From [6].

5. CyberCitz

The state of Virginia passed legislation in 2006 that a new component to the education curriculum for grades K-12 be included to implement instruction on Internet safety for students. The CyberCitz program was created by James Madison University to assist educators in integrating cybersecurity training into existing curricula [18]. The resources provided give teachers discussion topics, links to complementary websites and background information on security concepts. However, there is not much interaction that is created by the educator guide, between students and faculty. It serves as an informational guide, rather than a tutorial or training module to be utilized by an educator. As stated in the introduction of the guide, it is "organized in a way that addresses the ways middle-schoolers are using the Internet. It integrates ethical standards that can promote their use of the Web more wisely and responsibly." CyberCitz emphasizes topics like social networking and gaming which are applicable to these demographics. The concepts that CyberCitz discuss are very important to understanding major computer-security subjects that put Internet users at risk. An improvement on the "socialNetworking tutorial" could be to add interactive activities into the guide that actually have the class navigate through social networking sites to demonstrate protecting personal information. Students would benefit more from the CyberCitz lessons if there were interactive activities emphasizing the points described in each lesson. Rather than only focusing on classroom discussions or lectures. Below is an example lesson from the CyberCitz social networking lesson.

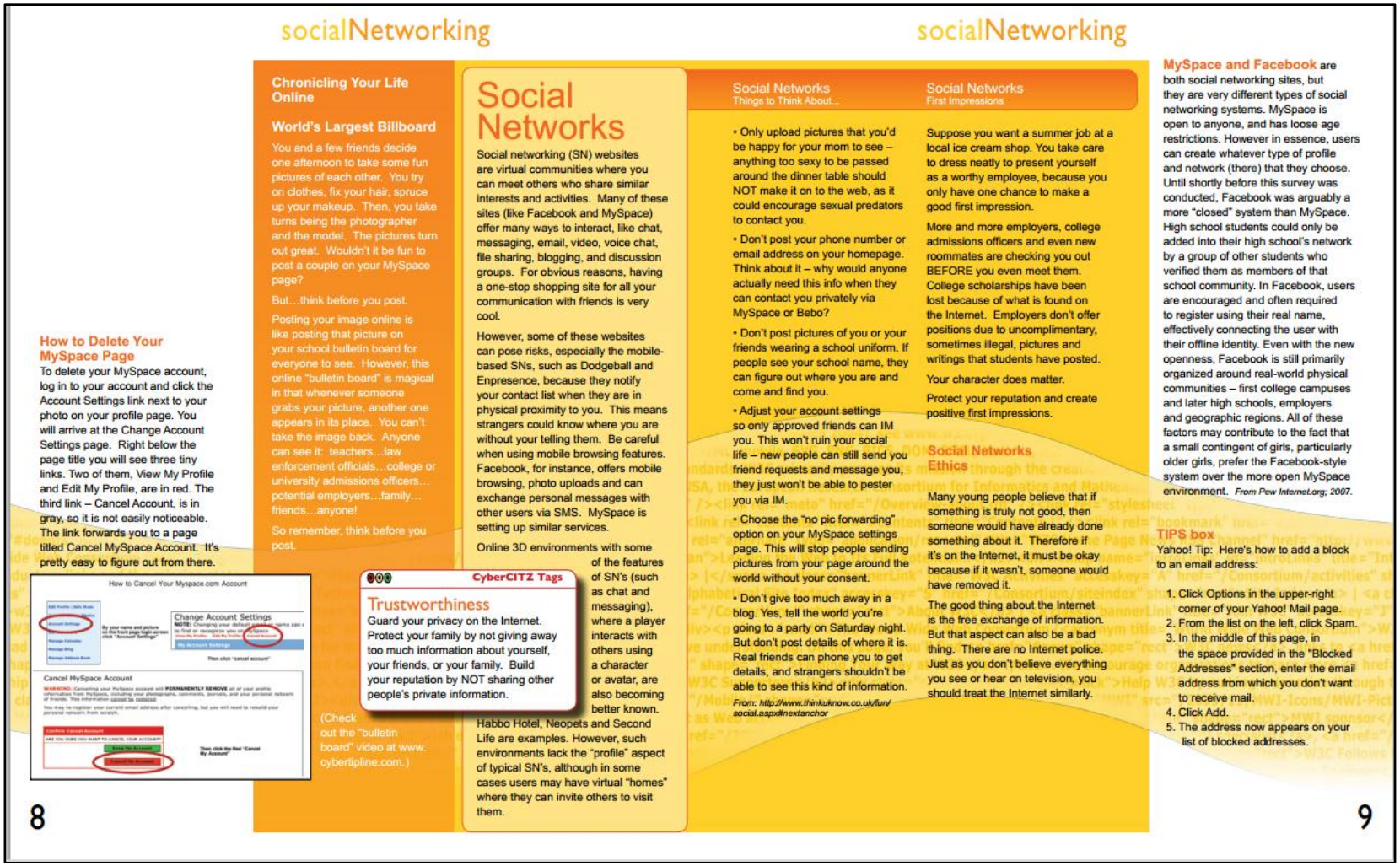


Figure 5. CyberCitz – Social Networking Lesson. From [18].

6. i-SAFE

i-SAFE is an electronic safety education program that was created to provide schools and school districts with curriculum materials and a variety of learning platforms. This curriculum provides teaching tools that have the goal of "equipping students with the critical thinking and decision-making skills they need to be safe, responsible and technologically proficient cyber citizens in today's global society and economy" [19]. This program was originally created as a nonprofit Internet safety organization in 1998 and subsequently has grown into providing over 34 million children with cybersecurity training. The curriculum for pre-primary to secondary schoolchildren covers an extensive number of topics from Cyber Community Citizenship (e.g., appropriate, safe and responsible online behavior) to Intellectual Property (e.g., ethical and legal use of online information, copyright regulations, etc.). In order to access this curriculum a subscription can be purchased for an individual school or for a school district.

A sample lesson plan provides a lesson guide, learning objectives, materials needed, and procedures for completing the lesson. Only three lesson plans are viewable on their website to those without a subscription. The curriculum outlines are similar to other programs reviewed. Only a small number of materials are used in the example curriculums, such as materials to create posters and activity pages to be filled out during class discussions.

Online Creativity and Ownership Lesson Sample:
Grades 9-12: Cyber Ethics and Peer-to-Peer Networks

LESSON—Cyber Ethics and Peer-to-Peer Networks

Suggested grade level 9-12

Lesson Guide

Learners will examine the concept of cyber ethics and how ethics apply within the peer-to-peer network environment.

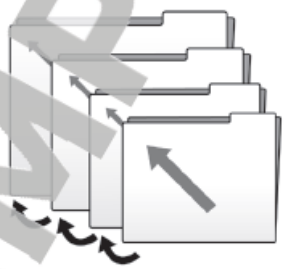
Learning Objectives

Students will:

- understand the term file-sharing and its uses
- understand the term cyber ethics
- understand the ethical issues associated with file-sharing, including intellectual property

Materials/Preparation

- a copy of reference and activity pages for each student



Procedures

Discussion

Begin discussion with the following open-ended questions:

- What are laws? How do laws guide how we behave from day to day?
- How do laws govern our online actions?
- What are ethics? How are they similar to laws? How are they different?
- Ask students to define ethics.
- Ask students how ethics can/should govern our online actions.

Reference Page:

- Hand out the reference page to students and discuss.
- Divide students into small groups to complete the "Think About It" section.
- Meet back as a class to discuss group answers.

Activity

- Break students into small groups.
- Tell students the question of the day is: What are your cyber ethics?
- Explain that their activity today is to create a list of five to 10 "ethic" statements to guide Internet use and usage of peer-to-peer networks. During the creation of these, keep in mind the definition and key goal of ethics: to do no harm within the global society, Cyberspace.

Figure 6. i-SAFE Cyber Ethics Lesson for Grades 9–12. From [19].

C. FEDERAL GOVERNMENT CYBERSECURITY TRAINING PROGRAMS

1. Stop.Think.Connect

In 2009, when Obama required a cyber-security federal policy review, the Department of Homeland Security created an initiative called "Stop.Think.Connect" [20]. This campaign created a coalition in an effort to encourage much needed Federal agency and SLTT government leadership involvement "to promote awareness about cyber threats and online safety practices both within their organizations and to the general public" [20]. Out of this collaboration has grown a partnership between different levels of the U.S. government and other national cyber-security campaigns to promote cyber-security training of children. The groups affiliated are:

- National Crime Prevention Council
- National Cyber-security Alliance
- Netsmartz – a program of the National Center for Missing and Exploited Children (NCMEC).
- Cyber-security Awareness Volunteer Education (C-SAVE)
- Federal Trade Commission's (FTC) OnGuard Online.
- United States Computer Emergency Readiness Team (U.S.-CERT)

The Stop.Think.Connect campaign is not a curriculum but an initiative to spread information about Internet safety. It provides tip sheets and other quick reference resources for children and parents to learn about safe Internet usage. In contrast, there are federal cyber-security training programs for children. Each of the programs are outlined in the following sections.

Keep a Clean Machine.

- **Keep security software current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option..
- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information.

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Connect with Care.

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- **Protect your $$:** When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

Be Web Wise.

- **Stay current. Keep pace with new ways to stay safe online.** Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

Figure 7. Stop.Think.Connect "Tips and Advice" Sheet. From [20].

2. StaySafeOnline.org

The United States' National Cybersecurity Alliance has created the StaySafeOnline.org, devoted to "educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets" [21]. Like

ACMA's Cybersmart, NCA's StaySafeOnline uses classroom activities, scenario discussions and games to illustrate cyber concepts. StaySafeOnline also uses a fictional story, written by Jacalyn S. Leavitt, called "Faux Paw the Techno Cat: Adventures in the Internet." This story is a visual tool that teachers can use to reemphasize concepts learned in classroom activities. StaySafeOnline has similar functionality as its Australian counterpart, Cybersmart. It accumulates existing resources into one website where parents, teachers, and administrators can use them to teach cyber-security. This includes a K-12 resource report, listing the nation's leading cyber-security training programs and teaching resources for group delivery(Figure 14 in Appendix).

Three different sets of teaching materials were created for different age groups K-2nd grade, grades 3–5, and Middle & High School. Each age group has a different set of learning objectives:

a. Grades K–2:

- It is essential that students understand and commit to not sharing personal information with anyone they meet online.
- Reinforce that children should talk openly with their parents or guardian about what they see online and should always tell them if anyone asks for personal information.
- Students must commit to follow the family and school rules about safety on the Internet and when playing online games.

b. Grades 3–5:

- It is essential that students understand and commit to not sharing personal information with anyone they meet online. This includes their real name, address, phone number, financial information, school name, passwords, or other private information.
- Reinforce that children should talk openly with their parents or guardian about what they see online and should always tell them if anyone asks for personal information or makes them feel uncomfortable.
- Students must commit to follow the family and school rules set up to keep everyone safe while online.

c. Middle and High School:

- It is essential that students understand and commit to not sharing personal information with people they view as "friends" online. This includes their real name, address, phone number, financial information, school name, passwords, or other private information.
- Although many students at this age level know basic ways to stay safe while online, they must also commit to ethical online users. Simple items to review include:
- Post only what you would feel comfortable with the whole world seeing, including parents or college admissions personnel.
- Never use the Internet to spread gossip, bully or hurt someone's reputation.
- Students should understand what security tools are available to use on most computers to further protect themselves, their personal information, and their computer from viruses, spyware, and spam.
- Students must also understand that they are in charge of their online experience and should manage it the way they would in the real world. If something or someone online makes them feel uncomfortable, they have the right to not respond, delete a post, and most importantly tell a trusted adult.
- Students must commit to never meet in person with someone they met online.

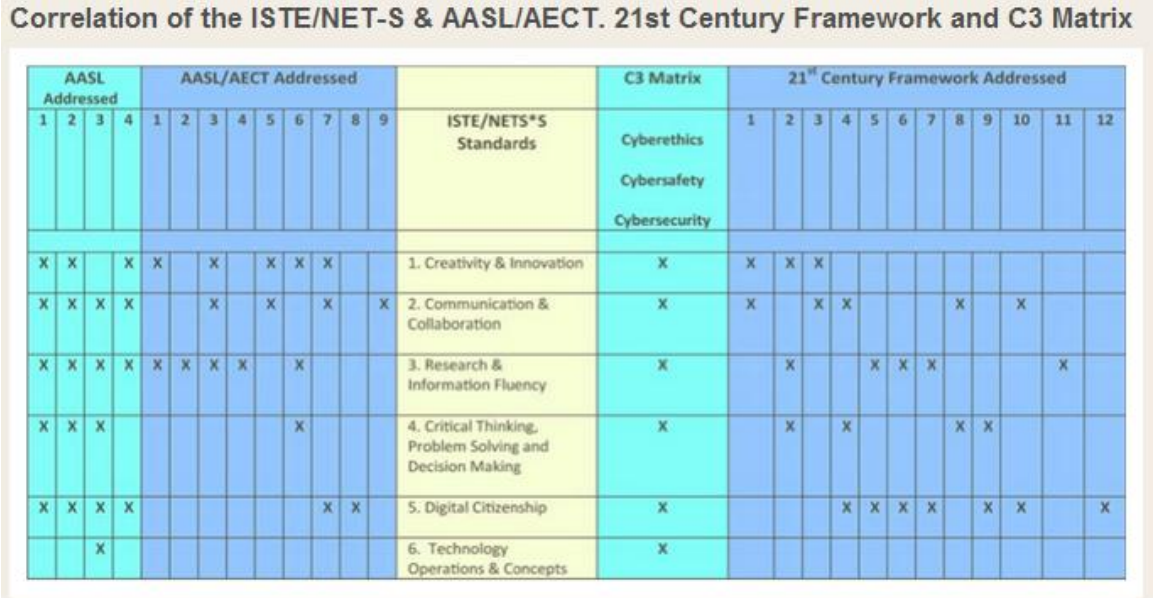
3. iKeepSafe

The Internet Keep Safe Coalition "is a broad partnership of governors and/or first spouses, attorney generals, public health and educational professionals, law enforcement, and industry leaders working together for the health and safety of youth online" [22]. The "iKeepSafe" program [23] is an educational online resource that helps train educators, parents, administrators, and students about cyber-security and safety. There a four programs in the iKeepSafe suite of tools to deliver cyber-security training. The first program is "iKeepCurrent" which is a newsfeed that is a "constant source of headline-inspired curricula and professional development mixed with fresh, entertaining content" to be utilized as discussion topics between educators and students. Secondly, "Generation Safe" is a tool that provides resources to help the "whole school community navigate the digital environment by providing a comprehensive set of resources for all stakeholders;

professional development (training), incident management, and a comprehensive self-assessment." The "Faux Paw" cartoon series is a devised curriculum that is meant for elementary school children. Teachers have access to books, animated DVDs and lesson plans that are supplementary to the cartoon series.

Figure 8. Faux Paw, The Techno Cat; StaySafeOnline.org. From [23].

The C3 matrix below is a tool that educators can use that makes iKeepSafe's program a little different than other national programs. This matrix assists teachers in integrating three essential concepts into their existing technology or other type of curricula. The matrix is subdivided into three competency levels for specific subjects; basic, intermediate, and proficient.



Correlation of the ISTE/NET-S & AASL/AECT. 21st Century Framework and C3 Matrix

AASL Addressed				AASL/AECT Addressed									ISTE/NETS*S Standards	C3 Matrix	21st Century Framework Addressed										
1	2	3	4	1	2	3	4	5	6	7	8	9		Cyberethics Cybersafety Cybersecurity	1	2	3	4	5	6	7	8	9	10	11	12
X	X		X	X		X		X	X	X			1. Creativity & Innovation	X	X	X	X									
X	X	X	X			X		X		X		X	2. Communication & Collaboration	X	X		X	X				X		X		
X	X	X	X	X	X	X	X		X				3. Research & Information Fluency	X		X			X	X	X				X	
X	X	X							X				4. Critical Thinking, Problem Solving and Decision Making	X		X		X				X	X			
X	X	X	X							X	X		5. Digital Citizenship	X				X	X	X	X		X	X		X
		X											6. Technology Operations & Concepts	X												

Figure 9. Matrix Table for Implementation into current curricula. From [22].

4. Netsmartz

The Netsmartz program was created by the National Center for Missing & Exploited Children (NCMEC) "that provides age-appropriate resources to help teach children how to be safer on- and offline. The program is designed for children ages 5–17, parents and guardians, educators, and law enforcement. With resources such as videos, games, activity cards, and presentations, NetSmartz entertains while it educates" [24]. Goals of the program are outlined as follows:

- Educate children on how to recognize potential Internet risks
- Engage children and adults in a two-way conversation about on- and offline risks
- Empower children to help prevent themselves from being exploited and to report victimization to a trusted adult

Furthermore, educators are provided the opportunity to utilize teaching materials that are specifically created to facilitate education of different age groups. These groups span age ranges 5–7, 8–10, 11–13, 14–17, and Adult. Teachers are recommended to use the materials by first identifying the age group that they wish to teach and then the specific Internet safety topics they wish to implement into their current curriculum. Netsmartz addresses the following topics: Cyberbullying, Inappropriate content,

Predators, Revealing too much Information, Spyware, spam, and scams. Each one of these primary topics has sub-topics that educators can utilize to be more specific.

Netsmartz uses a variety of teaching materials for each sub-topic: Videos, activity cards, teachable recipes, Internet safety rules, Internet safety presentations, and handouts/activity worksheets. In the Appendix, Figure 15 is an example discussion sheet about "Information Hiding" for the 5–7 age group. Figure 16 is an activity sheet about "Basic Internet Safety" for the next age group, Intermediate (ages 8–10).

5. State Government Cyber-security Curriculum Standards

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a cyber-security collaboration among all fifty states. The mission of the MS-ISAC is "to improve the overall cyber-security posture of state, local, territorial and tribal governments. Collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security are the keys to success" [25]. This organization grew out of a small contingent of Northeastern states into being designated by the DHS as the primary means of information sharing. Their role is primarily centered on providing two-way sharing of information and early warnings on cyber-security threats between states. Another important objective is that they are vested in helping to coordinate training and awareness between the states. However, they only provide links to national training programs and do not actually endorse any of the resources.

Some states are cognizant of the need for cyber-security training at all education levels. In February 2012, Ohio conducted a cyber-security review that produced a cyber-security awareness program that utilizes the NICE framework [26]. The state of Virginia's Information Technologies Agency (VITA) created "awareness" webpages that provide cyber-security resource links to its citizens. Going even further, the state of New York created a program that is to be implemented into all state education curricula.

a. NYS Education Law–Section 814: Courses of Study in Internet Safety

Below is an excerpt from the enacted New York State education law that was passed into law in 2010. This law is an example that ten states have enacted as a result of the Federal Cyber Initiative.

- Any school district in the state may provide, to pupils in grades kindergarten through twelve, instruction designed to promote the proper and safe use of the Internet.
- The commissioner shall provide technical assistance to assist in the development of curricula for such courses of study which shall be age appropriate and developed according to the needs and abilities of pupils at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the Internet.
- The commissioner shall develop age-appropriate resources and technical assistance for schools to provide to students in grades three through twelve and their parents or legal guardians concerning the safe and responsible use of the Internet. The resources shall include, but not be limited to, information regarding how child predators may use the Internet to lure and exploit children, protecting personal information, Internet scams and cyber bullying.

New York State subscribes to the "Stop.Think.Connect," the Infinite Learning Lab, NetCetera, NCMEC, iKeepSafe campaigns as their primary resources for educators to provide cyber-security topics and training to their students.

D. SUMMARY

In this chapter, we presented examples of cyber-security curricula for non-technical persons. We have displayed the current techniques educators are using to teach children and others with non-technical backgrounds important computer-security concepts. We will use accreditation standards of national teaching programs to assess multiple traits of each "state of the art" program presented above. By using the best features of each lesson, we hope to provide recommendations for the implementation and development of a syllabus that is most conducive for non-technical people to learn cyber-security.

III. CURRICULUM FRAMEWORK

In this section, we will present the design and format metrics as prescribed by national curriculum accreditors for a primary and secondary-school curricula. We will present ways that other STEM curricula have been developed and what the standards are for an accreditation of a national curriculum. In the previous chapter we have discussed the current body of knowledge for teaching computer-security concepts and principles in primary and secondary education. Each program is slightly different in its development and how it appeals to students. Our objective is to develop a set of standards that allow an educator to assemble the best characteristics of every curriculum into their own tailored set that is most effective for their classroom.

Our work will strive to answer the following questions:

- What pedagogical techniques and tools have been identified as the best for communicating cyber-security topics to a target audience of children, grades K-12?
- What metrics are used to measure the effectiveness of these curricula?
- What topics are currently missing or deficient in the existing literature, are these topics important, and how can we overcome these deficiencies?
- How are children effectively trained in a subject of which they have no prior knowledge?

Our research work will also incorporate teaching strategies that have been utilized in other technical areas as well as computer-security. For example, the University of Wisconsin created a teaching aid that allows teachers of STEM topics to "most effectively teach difficult concepts" [27]. This aid discusses the use of the following techniques: case studies, open-ended labs, open-ended quizzes, brainstorming, question-and-answer methods (i.e. Socratic), and practical examples. Many of their students expressed concern regarding the need for more industrial and practical examples "to reinforce theory with practical applications" [27]. The same could be applied to illustrating technical security scenarios when teaching an unfamiliar audience. Even though this teaching aid was created for the development of undergraduate curricula, many of the strategies are applicable to a younger audience when developing a computer-security program:

- Practical Examples-These examples will be used to connect computer-security theory with practical applications or real-world examples in order to help illustrate more effectively topics that are not as transparent.
- Case Studies–Bringing real scenarios into the classroom as tangible evidence of topics. Cases could involve a number of concepts and could be used to tie in a number of sub-topics at the end of a module.
- Open-Ended Quizzes–These can be used to stimulate student's creativity and to help students think beyond just new vocabulary.
- Brainstorming–This technique is widely used to for an audience or class to generate their unique ideas about a sub-topic. This allows students to work together and add in their personal experiences to help illustrate or analyze a problem.
- Question-and-answer Method–This will encourage students to actively participate through a Socratic method, rather than focusing on memorization, students are then encouraged to answer questions at the end of each sub-topic and module. This will stimulate more clarification, expansion, generalization, and applicability of every subject.

Utilizing effective teaching strategies for technical subjects will be just as important as creating the syllabus. "As you plan to teach a subject, you must remember that the processes that students use to master the content of a lesson are just as important as the content itself" [28]. For example, a teaching instruction could be created for a subject like "'integrity"' to be presented to a group of children. The topic will be unique to the audience, since this might be the first time that they have been introduced to the subject matter. This then allows for an evolution of the curriculum to occur. A proctor will be able to be innovative in the way they present the information, and therefore can consider different teaching approaches that will produce more effective lessons dependent on the class.

The intent is to gather all of the best tools of creating teaching theories and then to apply them to main ideas of computer-security. To reiterate, the main thrust of this study has been to investigate the current status of children's information assurance (IA) and computer-security education. In a 2009 survey paper titled "An Exploration of the Current State of Information Assurance Education," Cooper et al. conclude, "Due to the relative newness of the field of study, to date, no accrediting body specifically considers or examines IA as an independent program of study" [29]. Currently, there is no formal

accreditation for private-sector or IA programs. However, four-year colleges and graduate-level universities can be certified as a member of The National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) Program. The CAE/IAE Program is jointly sponsored by the National Security Agency and the Department of Homeland Security. To become a CAE/IAE, an institution must "go through a rigorous two-phase evaluation process." There has not been a similar focus applied to elementary or secondary computer-security programs.

The crux of teaching cyber-security education is being able to convey technical concepts in a concise and entertaining way to an elementary user. For the purposes of this work, we define a non-technical user as a person with either no or minimal exposure to computer-security concepts, and who does not believe they use computers in their daily lives more than average. According to the National Association for the Education of Young Children (NAEYC), "[G]ood teaching begins with knowing the learners – what they are like developmentally, individually, and culturally" [30]. The NAEYC is the largest nonprofit association in the U.S. representing early childhood education teachers, paraeducators, center directors, trainers, college educators, families of young children, policy makers, and advocates [30]. Their goals are centered on promoting excellence in childhood education programs throughout the U.S. Their accreditation process is very stringent and is highly regarded throughout the nation. Since NAEYC sets the standard for educational/curriculum standards in the U.S., we use their standards to inform any model for effective cyber-security programs for children.

1. Curriculum Standards

We present our findings in a clear and concise manner that is centered on a pedagogical survey of cyber-security education. After having completed a review of many of the top cyber-security education programs, through close examination we present the best traits of each based on the educational standards of the NAEYC, the Association for Middle Level Education (AMLE) [31], and the National Science Teachers Association (NSTA) [32]. In order to be an accredited program, a curriculum must satisfy the following criteria: [31], [32], [33].

- The program has a written statement of philosophy and uses one or more written curricula or curriculum frameworks consistent with its philosophy that address central aspects of child development.
- A clearly stated curriculum or curriculum framework provides a coherent focus for planning children's experiences. It allows for adaptations and modifications to ensure access to the curriculum for all children.
- The curriculum guides teachers' development and intentional implementation of learning opportunities consistent with the program's goals and objectives.
- The curriculum can be implemented in a manner that reflects responsiveness to family home values, beliefs, experiences, and language.
- Curriculum goals and objectives guide teachers' ongoing assessment of children's progress.
- The curriculum guides teachers to integrate assessment information with curriculum goals to support individualized learning.
- The curriculum guides the development of a daily schedule that is predictable yet flexible and responsive to individual needs of the children. The schedule provides time and support for transitions.
- Includes both indoor and outdoor experiences.
- Is responsive to a child's need to rest or be active.
- Materials and equipment used to implement the curriculum reflect the lives of the children and families as well as the diversity found in society including:
    - Gender
    - Age
    - Language
    - Diversity of Abilities
    - Materials and Equipment
- Provide for children's safety while being appropriately challenging.
- Encourage exploration, experimentation and discovery.
- Promote action and interaction.
- Are organized to support independent use.
- Are rotated to reflect changing curriculum and accommodate new interests and skill levels.
- Are rich in variety.

- Accommodate children's special needs.
- Materials and equipment used to implement the curriculum for infants and toddlers/twos encourage:
    - exploration, experimentation, and discovery.
    - sensory and motor learning.
    - practice of developing physical skills through self-initiated movement.
- The curriculum guides teachers to incorporate content, concepts, and activities that foster:
    - social [development],
    - emotional [development],
    - physical [development],
    - language [development], and
    - cognitive development and
    - integrate key areas of content including literacy, mathematics, science, technology, creative expression and the arts, health & safety, and social studies.
- The schedule provides children learning opportunities, experiences, and projects that extend over the course of several days and incorporates time for play, creative expression, large-group, small-group, and child-initiated activity.
- The curriculum guides teachers to plan for children's engagement in play (including dramatic play and blocks) that is integrated into classroom topics of study.

These are the objectives that are necessary for curriculum development but there are other facets of teaching children that are important for a student's overall development and complete understanding of a topic. The NAEYC has grading criteria that emphasizes physical and cognitive development in the following areas: literacy, mathematics, science, technology, and social studies. Not every one of the criteria guidelines is relevant to our research, but each one has an important approach to teaching children different subjects.

2. Curriculum Objectives

Examples of syllabus development for young children are centered on incorporating a variation of teaching strategies. I.e., there are a variety of ways that a teacher can present the same topic to a class. The NAEYC [33] and the International Society for Technology in Education (ISTE) [34] give different examples of how to most effectively teach science subjects to children ranging from preschool through twelfth grade. The following are features of what a 'successful implementation' by ISTE standards [35], AMLE standards [31], NSTA standards [32], and a NAEYC 'accredited' computer curriculum [33] should use and select:

- **Environmental Design.** [33] The curriculum should organize space and select material in all content and development areas to stimulate exploration, experimentation, discovery, and conceptual learning. The intent of this criterion is that teachers will be intentional when organizing and presenting materials in the classroom.
- **Clearly Stated Learning Objectives**. Does the curriculum clearly state the learning objectives for each lesson? Teachers should clearly discuss the purpose of each lesson so that students are aware of required material covered on future assessments.
- **Engaging Activities.** Teachers should use multiple methods to deliver curricular materials, including in-person and web-based social and content-delivery mechanisms. One example is for students to critically think through a scenario, by providing solutions to the class when prompted by the teacher. By allowing students to demonstrate their own personal experiences, students will more quickly adapt to new subjects and be able to pull from requisite knowledge [33], [35]. The curriculum should utilize websites for independent student activities (self-guided, fun, non-teacher-directed). Are teachers using simulations or models in their teaching to help kids understand and appreciate difficult sub-topics [35]?
- **Classroom Displays.** Teachers should create Classroom Displays that help children reflect on and extend their learning. They should ensure that children's recent works predominate in Classroom Displays (e.g., art, emergent writing, graphic representation, and three-dimensional creations.) Predominate means appears in the majority or in more than half of the displays. One or more display areas are at children's eye level [33].
- **Reaffirmation/Reiteration of Topics.** Teachers plan for children to revisit experiences and materials over periods of days, weeks, and months. Evidence of this could include lesson plans, planning webs, photos, etc. Activities around a thematic unit or a set of materials that last for several

days, then continue at intervals for weeks or months [33]. By revisiting the topic, a teacher can ensure the comprehension of a sub-topic that is important to an overall objective or theme.

- **Organization of Time and Space.** Teachers organize time and space on a daily basis to allow children to work or play individually, in pairs, to come together in small groups, and to engage as a whole group. By creating opportunities for children to engage in group projects, teachers are intentionally promoting children's ability to learn from each other [33].
- **Create Experiences in Response to Children's Interests and Needs.** Teaching staff reorganize the environment when necessary to help children explore new concepts and topics, sustain their activities, and extend their learning. Teachers' scaffold children's learning by modifying the schedule, intentionally arranging the equipment, and making themselves available to children. Also, teachers should use children's interest in and curiosity about the world to engage them with new content and developmental skills [33].
- **Teachers Demonstrate Knowledge.** Teachers demonstrate their knowledge of content and development areas by creating experiences that engage children in purposeful and meaningful learning related to key curriculum concepts. These can include created experiences based on spontaneous activities that emerge from a planned activity. Teachers could demonstrate technology by the actual use of machines and tools. Technology can be used by teachers or children in dramatic play [33] [35].
- **Assessment Plan.** The program has a written plan for assessment that describes assessment purposes, procedures, and uses of the results. The plan should include conditions under which children will be assessed, timelines associated with assessments that occur throughout the year, ways to involve families in planning and implementing assessments, and methods to effectively communicate assessment information to families. Assessment methods should be aligned with curriculum goals, provide an accurate picture of all children's abilities and progress, are appropriate and valid for their stated purposes, provide meaningful and stable results for all learners, provide teachers with clear ideas for curriculum development and daily planning, and are regularly reviewed to be certain that they are providing the needed information [33].

These standards will be the benchmark for our survey of the widely-used cyber-security programs that were introduced. We will use these standards as objectively as possible when surveying each program.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SURVEY RESULTS OF CURRENT COMPUTER-SECURITY PROGRAMS

In the following pages we summarize our survey research of all the cyber-security programs for grades K-12. There are a total of nine major programs, introduced above in Chapter 2, that are applicable to this demographic.

Each of the following nine programs were graded according to the NAEYC curriculum standards iterated above: Environmental Design, effective transition of subjects, Engaging Activities, Classroom Displays, Reaffirmation/Reiteration of Topics, organization of time and space, created experiences in response to children's needs, teacher demonstrates knowledge, and creation of an assessment plan. Each standard will be evaluated by being given a score of 0 to 2 by increments of one. The score will be listed after each title.

- A grade of 0 implies that the program has no examples of this standard.
- A grade of 1 implies there are only limited examples of this standard.
- A grade of 2 implies there are strong examples of this standard.

An overall score of each curriculum is tallied after completing a survey. This score only represents how well a program followed specific traits of a NAEYC certified educational program. Each score will be compared at the completion of this chapter.

A. CERIAS

Environmental Design**: 2**

CERIAS presents a wide variety of computer-security topics in its curriculum. There is a sufficient amount of material that could be referenced and applied to elementary-school and middle-school students. There are a total of 14 topics that are a part of the overall computer-security curriculum. Each topic is aligned with "Indiana Academic Standards" so that teachers know their lesson is emphasizing the school's overall curriculum goals.

Clearly Defined Learning Objectives: 2

Each lesson starts with a list of learning objectives that the teacher should explain and focus on when presenting the information.

Engaging Activities: 2

There are mandatory activities and supplemental activities that are listed on each topic's worksheet. Procedures, required materials and closure discussion topics are also itemized in each lesson guide.

Classroom Displays: 2

There are no visual aids that are provided as a part of the curriculum. However, during some lessons, students are encouraged to make posters and then to display them near computers in the classroom. When students create posters in conjunction with their lessons, they are used to emphasize the main subjects, i.e., instant messaging—information protection. Students are asked re-create a subject with their own representations of what a topic means to them [33].

Reaffirmation/Reiteration of Topics: 0

There is no evidence that the presentation of topics should be revisited or approached in an alternate way. The lesson plans are autonomous that are not a part of a grander schedule or syllabus.

Organized Time and Space: 2

Each lesson plan clearly defines all necessary materials and actions by the teacher and students.

Created Experiences in Response to Child's Needs: 1

The importance of classroom discussions and individual activities are reinforced in most of the lesson plans. If a child might require more instruction, then supplementary websites or activities are suggested for further exploration.

Teachers Demonstrate Knowledge: 1

Teachers are expected to facilitate classroom discussions and to engage students during each of the required activities. In the curriculum description, teachers are given guides and are encouraged to attend curriculum workshops that are conducted by the CERIAS program facilitators.

Assessment Plan: 0

There was no assessment plan associated with the program.

Overall Program Score: 12

B. CS UNPLUGGED

Environmental Design: 2

CS Unplugged is a curriculum that teaches approximately twenty-two computer science topics. The curriculum is uses many different aspects of the classroom or group dynamics to present a topic. Environmental design is about the use of the classroom environment and its materials. CS Unplugged is very conscious about how it uses physical space, and the presentation and order of concepts and materials. A teacher is not restricted by the curriculum, as far as how they want to present the lessons and activities to the students. The design is very flexible and accommodating to the full spectrum of classroom types and capabilities.

Clearly Defined Learning Objectives: 1

Each lesson lists a “focus” of the activity, but they are not described in any further detail than a one-word description or a phrase. When a teacher uses the teaching materials, there is more description of the goals for each topic. The teachers and students would be served well by being given further explanation of the purpose of an activity. That way more parallels could be drawn and a teacher might more easily incorporate a lesson into their normal curriculum plans.

Engaging Activities: 2

The lessons explain one activity for each topic. They allow a small or large group to participate. These groups are required to cooperate to complete a lesson or activity. The groups strive to answer a topical question by participating in kinesthetic game-like exercises. Each activity prescribed is accomplished with only a limited number of easily accessible materials.

Classroom Displays: 1

CS Unplugged doesn't offer any classroom displays or materials that can be used to integrate into the classroom environment. Teachers are encouraged to keep examples of the materials that the students create after each lesson. That way they can be used as reference in the future or can be displayed as reminders of lesson topics.

Reaffirmation/Reiteration of Topics: 1

Included on CS Unplugged' website is a link to the Computer Science Teachers Association (CSTA) that is meant to provide teachers ideas of how to integrate CS Unplugged activities into their own curriculum. However, there are some suggestions of specific activities that could be integrated with other math or science learning objectives.

Organized Time and Space: 2

The activities presented in the curriculum specify how much time is required for completion. Materials that are needed for the activity are explicitly stated on each worksheet. Most of the materials required are minimal and can be completed in any classroom environment. The uniqueness of CS Unplugged is very evident since there are no physical restrictions that are placed on the teacher or student.

Created Experiences in Response to Child's Needs: 2

In the teacher's edition book provided, each activity is presented clearly for the teacher to utilize. Also, each activity is associated with a "Curriculum Link" that a teacher can use to incorporate into normal lesson plans. If a class or individual student has already mastered the activity then there is an "Extra for Experts" section at the bottom of each activity that provides further instruction for more gifted students.

Teachers Demonstrate Knowledge: 2

Each teacher is required to be very familiar with each activity before they present it to the class. There are discussion sections at the beginning of each worksheet and they are supposed to provide a direction of discussion for the entire class. Prior preparation is necessary by each teacher in order to be able to answer general questions about the structure of each activity and what each student is expected to understand by their actions.

Assessment Plan: 1

There are no assessments offered by the curriculum. A teacher would have to make up an assessment from the discussion questions and activities provided by CS Unplugged. Completion of each activity does require an understanding of the information being presented in each module. If a teacher is accurately tracking a student's answers to the questions, then a student's comprehension of the material could be determined.

Overall Program Score: 14

C. CYBER(SMART:)

Cyber(smart:) presents a wide variety of computer-security topics in its curriculum. There is a sufficient amount of material that could be referenced and applied to elementary-school and middle-school students. There are a total of 11 topics that are a part of the overall computer-security curriculum. Not every topic is meant for each age-group. For example, younger students do not discuss the "sexting" topic, while older students are not exposed to the topic "Sharing personal information." Each topic is aligned with "Australian Academic Standards" so that teachers know their lesson is emphasizing the school's overall curriculum goals. The curriculum could be expanded further to discuss other computer-security topics. Safe social networking practices are the main focus of the curriculum for students' ages 16 years old and up.

Environmental Design: 2

The design of the curriculum is very conducive to use in a variety of types of classrooms. Many of the lessons utilize different types of multimedia for presentation. These include the curriculum website, PowerPoint, in-class worksheets, and videos.

Teachers can also present a lesson with only physical materials, like the worksheet and any materials needed to complete an activity.

Clearly Defined Learning Objectives: 2

Each lesson lists clear objectives for each activity. "Aims" are a description of the lesson and the subjects it is trying to convey. "Objectives" are what students are expected to comprehend following the completion of each lesson.

Engaging Activities: 2

The lessons explain one activity for each topic. They allow a small or large group to participate. Each activity prescribed is accomplished with only a limited number of easily accessible materials. Students are meant to use multimedia resources and common classroom tools to complete each worksheet.

Classroom Displays: 2

Cyber(smart :) offers a variety of classroom displays like posters, and banners that can be hung around computer stations. As well, many of the activities require students to produce a physical result. Completed activities can be displayed in the classroom for future reference by each student.

Reaffirmation/Reiteration of Topics: 1

Included on CS Unplugged' website is a link to the Computer Science Teachers Association (CSTA) that is meant to provide teachers ideas of how to integrate CS Unplugged activities into their own curriculum. However, there are some suggestions of specific activities that could be integrated with other math or science learning objectives.

Organized Time and Space: 2

The activities presented in the curriculum specify how much time is required for completion. Materials that are needed for the activity are explicitly stated on each worksheet. Most of the materials required are minimal and can be completed in any classroom environment. The uniqueness of CS Unplugged shows through since there are no physical restrictions that are placed on the teacher or student.

Created Experiences in Response to Child's Needs: 2

In the teacher's edition book provided, each activity is presented clearly for the teacher to utilize. Also, each activity is associated with a "Curriculum Link" that a teacher can use to incorporate into normal lesson plans. If a class or individual student has already mastered the activity then there is an "Extra for Experts" section at the bottom of each activity that provides further instruction for more gifted students. Teachers also have a link on the program's website for lesson plans that can be used for children with special education needs.

Teachers Demonstrate Knowledge: 2

Each teacher is required to be very familiar with each activity before they present it to the class. There are discussion sections at the beginning of each worksheet and they are supposed to provide a direction of discussion for the entire class. Prior preparation is necessary by each teacher in order to be able to answer general questions about the structure of each activity and what each student is expected to understand by their actions.

Assessment Plan: 0

The curriculum offers no assessment plan for the teacher delivering the material. Each worksheet has discussion questions listed but there is no plan implemented to assess a student's overall understanding of the learning objectives/aims of the topic.

Overall Program Score: 15

D. CYBER SMART!

Environmental Design: 2

Cyber Smart! structures the curriculum around eight categories. The eight categories are: Internet safety, privacy & security, relationships & communication, cyber bullying, digital footprint & reputation, self-image & identity, information literacy, and creative credit & copyright. There are a total of fifteen lessons for each grade level from K-8th grade. There are twenty lessons for the high-school grades 9–12. Each lesson teaches either utilizes one or more of the eight major categories. Each of the units are

organized based on age-appropriateness of digital literacy and citizenship topics. The lessons also address community concerns by providing materials to educate parents, families, and community organizations.

Clearly Defined Learning Objectives: 2

Each lesson lists clear objectives for each activity. They are defined clearly by stating what each "will be able to" accomplish at the completion of each sub-topic instruction.

Engaging Activities: 2

Most of the activities are strongly balanced by utilizing media-rich lesson materials that emphasize skill-building, critical thinking, ethical discussion, media creation, and decision making.

Classroom Displays: 2

Cyber Smart! offers a small number of classroom displays already linked in the curriculum materials. Also, some of the sub-topics require the students to be divided into small groups in order to create posters for their classroom. Each poster is created to illustrate a theme they learned in a previous lesson. There are links to online videos and interactive web games that can be used to integrate into the classroom environment.

Reaffirmation/Reiteration of Topics: 2

The Cyber Smart! curriculum was created by including research-based lessons based on the work of Howard Gardner and the GoodPlay Project at the Harvard Graduate School of Education. Each of the learning objectives align with "Common Core State Standards, the International Society for Technology in Education's National Education Technology Standards (ISTE's NETS) and the American Association of School Librarians (AASL) Standards. Each of the activity worksheets lists the standards that are linked with the learning objectives. It is very easy for teachers to incorporate Cyber Smart! into their current lesson plans.

Organized Time and Space: 2

The activities presented in the curriculum specify how much time is required for completion. Materials that are needed for the activity are explicitly stated on each worksheet. Most of the materials required are minimal and can be completed in most classroom environments. A lesson can be taught with media or with only the most basic of classroom instruments.

Created Experiences in Response to Child's Needs: 2

In the teacher's edition book provided, each activity is presented clearly for the teacher to utilize. Also, each activity is associated with a "Curriculum Link" that a teacher can use to incorporate into normal lesson plans. If a class or individual student has already mastered the activity then there is an "Extension Activity" section at the bottom of each activity that provides further instruction for more gifted students.

Teachers Demonstrate Knowledge: 2

Each teacher is required to be very familiar with each activity before they present it to the class. There are discussion sections at the beginning of each worksheet which are used to provide a direction of discussion for the entire class. Prior preparation is necessary by each teacher in order to be able to answer general questions about the structure of each activity and what each student is expected to learn from the interaction.

Assessment Plan: 0

The curriculum offers no assessment plan. A number of worksheets for children in grades 9 through 12 are given about 3 short-answer questions after each activity. Other than discussion and direct questioning, the teacher has no other opportunity to gauge the knowledge of their students.

Overall Program Score: 16

E. CYBER CITZ

Environmental Design: 1

CyberCitz program offers a teacher's guide that has seven cyber-security topics that a teacher can use to implement into their own curriculum: general safety tips, digital

communications safety, social networking, emerging technology, surfing the web, video gaming, the dark side – cyberbullying. Each topic is covered by providing facts for the teacher to present to the class. Cyber Citizenship suggests a couple of different websites to visit that could more readily illustrate a specific topic. Only one-way communication from teacher to student is encouraged with this curriculum.

Clearly Defined Learning Objectives: 0

Each lesson topic has no learning objectives for the student. There is no definitive explanation of what each student should have learned upon completion of a module.

Engaging Activities: 0

There are no prescribed activities for the students participating in this curriculum.

Classroom Displays: 1

Cyber Citizenship offers posters and fliers that can be utilized by teachers to reinforce topics that they discussed in the curriculum. There are a total of six posters that illustrate the following themes of being a "cyber citizen": citizenship, trustworthiness, responsibility, caring, fairness, and respect. Students are not required to produce anything during any of the lessons. Chances for students to reflect on what they have learned through production of a tangible product are lost.

Reaffirmation/Reiteration of Topics: 1

The Cyber Citizenship curriculum has intended to create a website that would allow for further lesson plans and interaction of the topics discussed. During the research process, the website was still under construction and unable to be explored. Their curriculum guide provides links to other cyber-security training programs that could be used for further explanation of a topic if students require further instruction.

Organized Time and Space: 0

The topics presented in the curriculum do not specify how much time is required for completion. Materials that are needed for each topic are not explicitly stated on each worksheet.

Created Experiences in Response to Child's Needs: 0

In the teacher's edition book provided, each topic is illustrated by providing statistics about a topic. There is no variation of how a topic is supposed to be presented to the class. A teacher is only provided with material that can be delivered as a lecture. As well, student's prior knowledge of a topic is not taken into account nor can activities be adjusted for sub-average or advanced students.

Teachers Demonstrate Knowledge: 0

Only minimal preparation is required by the teacher to prepare for a topic. A teacher is only required to set aside time to read the lesson to the students. A teacher could prepare discussion questions based on the information, but is not required per the curriculum instruction.

Assessment Plan: 0

The curriculum offers no assessment plan. There are no knowledge checks of any kind in the curriculum.

Overall Program Score: 3

F. I-SAFE

Environmental Design: 2

The i-SAFE Corporation has created a curriculum that is composed of 362 lesson plans. Each lesson plan is meant for children ages 5 to 17 (grades K-12). The curricular design is further enhanced by a created flexibility that can accommodate different classroom environments, students with different learning abilities, and materials that assist in cross-curricular integration. Additional materials include: PowerPoint presentations, HTML activities, video webcasts, music songs via MP3 file, and other teacher resources.

Clearly Defined Learning Objectives: 2

Each lesson has concise learning objectives listed at the beginning of each activity. The curriculum states usually 3 or 4 objectives that a "student will" gain after completion of a topic.

Engaging Activities: 2

Most of the lesson plans include many different types of activities that support teachers in presenting cyber-security subjects. Types of activities include: visiting websites, videos, music sing-alongs, creation of a poster or brochure, building a bulletin board, answering short-answer questions, discussion questions, and class presentations.

Classroom Displays: 2

There are frequent opportunities for students to create Classroom Displays during many different topics in the i-SAFE curriculum. Examples include being asked to create a bulletin board about cyber-security. The "Acceptable Use Policies" unit requires students to create a brochure, poster, and a pledge exhibiting their understanding what cyber policies their school should enforce.

Reaffirmation/Reiteration of Topics: 2

The i-SAFE curriculum utilizes an "Implementation Strategy" document that is meant for teachers to use along with their current prearranged curriculum. This document can be used by teachers to decide how many hours of class time should be devoted to a topic, determine what activities will be used in that amount of time, and what topic lessons are most appropriate for a specific grade level.

Organized Time and Space: 1

The topics presented in the curriculum do not specify how much time is required for completion. A teacher can only approximate how long a lesson will take when they implement it into their current curriculum. Materials that are needed for each topic are explicitly stated on each lesson plan.

Created Experiences in Response to Child's Needs: 0

The curriculum guide does not discuss how each lesson plan can be tailored to a specific student's needs. There are some suggestions for tailoring the lessons for younger children in the "Implementation Strategy" guide, but there are no explicit instructions for teaching the concepts to below or above average students.

Teachers Demonstrate Knowledge: 2

Teachers are required to prepare for a topic by having ready all of the pertinent materials for each lesson. Review of each lesson is required so that a proctor is familiar with the concepts in the learning objectives. However, teachers are not required to have pre-requisite knowledge of the concepts before they commence a lesson. The "i-SAFE enrichment activities are designed so that they can be implemented by students."

Assessment Plan: 2

The curriculum offers an online assessment plan. There are online assessments that teachers can use after a completed lesson. Also, a database is maintained by i-SAFE Inc. to track students' understanding of the concepts presented. However, teachers are unable to track the individual efforts of students. The assessments are taken anonymously. A pre-assessment is taken prior to any i-SAFE lessons being conducted. A post-assessment is taken after all i-SAFE lessons are complete. Lastly, an outcomes assessment is taken 3–6 weeks following completion of the curriculum to "determine the core concepts that students retain over time" [19].

Overall Program Score: 15

G. STAYSAFEONLINE.ORG

Environmental Design: 1

The StaySafeOnline.org website is an online resource that is supposed to be utilized by individuals. The "I want to teach online safety," which is for teachers or community organizers, is very limited in its scope. The cyber-security curriculum has lesson plans that are tailored for 4 different age groups: Grades K-2, Grades 3–5, Middle & High School, and Higher Education. Each age group is provided with tools by this curriculum which includes: a lesson plan, a "Getting Started" introduction sheet, two class exercise/activities recommendation sheet, and answer sheet, and a class exercises report form. There is only one topic for every lesson plan in the curriculum: "becoming smart digital citizens ~using the C3 concepts and WWW checklist" [36]. The lesson plan is limited to only one cyber-security concept.

Clearly Defined Learning Objectives: 2

Learning objectives are clearly written on each lesson plan in the form of discussing the "overall purpose of your presentation and activities."

Engaging Activities: 1

Students are asked to participate in small and large-group discussions in each lesson. Activities are limited to question and answer activities. There are no other different types of classroom engagement prescribed in lesson plans.

Classroom Displays: 1

Posters are provided by the curriculum to be hung near computers as a reminder to students about cyber-security concepts.

Reaffirmation/Reiteration of Topics: 0

Each lesson is only meant to be completed once by each age group. There are no follow-up lessons.

Organized Time and Space: 2

The materials and time necessary for completion of each lesson are clearly listed at the beginning of each lesson plan. An example lesson plan is included in the appendix.

Created Experiences in Response to Child's Needs: 0

There are no special considerations for different audiences receiving the training.

Teachers Demonstrate Knowledge: 2

Teachers are required to prepare for each lesson since they are conducting the discussions. Also, lesson plans come with a "Getting Started" sheet this supposed to help facilitate the lesson with probing questions about cyber-security scenarios or concepts.

Assessment Plan: 0

At the end of each lesson, teachers are reminded to probe students with questions about the concepts they learn. However, there is only a suggestion to reiterate the lesson if a student is unsure of an answer. There is no formal test in place to gauge the students' comprehension of the lesson topics.

Overall Program Score: 10

H. I-KEEPSAFE

Environmental Design: 1

The iKeepSafe website is an online resource that parents or teachers can use to teach cyber-security concepts. Online resources are presented on the website to be used in conjunction with current technology and literacy curricula. There is a C3 matrix that is provided "to assist educators in integrating the essentials of cyber-safety, cyber-security, and cyber-ethics (C3 concepts) into existing technology and literacy standards and curricula" [23]. Other cyber-security-related resources include links to a "Google Digital Literacy Tour," an IT training resource for school administrators called "iKeepSafe Generation Safe," and "Project PRO," a partnership to be used between schools and digital companies. The iKeepSafe organization does offer a formal curriculum in the form of the "Faux Paw the Techno Cat," that can be used for cyber-security training of younger children. This curriculum is only recommended for children ages 5–12.

Clearly Defined Learning Objectives: 2

Each lesson plan lists the learning objectives at the beginning of each worksheet.

Engaging Activities: 2

The Faux Paw curriculum uses supplementary materials like videos, books, powerpoints, and activity worksheets to present C3 concepts. Children are engaged by conducting classroom discussions with the teacher and are given multiple opportunities to utilize different types of media during each lesson.

Classroom Displays: 2

The curriculum offers posters that can be displayed near computers to reaffirm C3 concepts discussed in the Faux Paw lessons. Teachers can also hang completed worksheet activities by the students to remind them of important topics or themes from specific lessons.

Reaffirmation/Reiteration of Topics: 2

There are multiple lessons that can be used in conjunction with current lesson plans. The Faux Paw curriculum lists "curriculum connections" that are used by teachers to incorporate a specific lesson into their school's already approved curriculum schedule.

Organized Time and Space: 2

Most of the lesson worksheets describe the amount of time and materials that are needed to complete each lesson.

Created Experiences in Response to Child's Needs: 0

The Faux Paw curriculum does not discuss how the lessons could be tailored for a specific child's needs.

Teachers Demonstrate Knowledge: 1

Teachers are expected to be able to facilitate classroom discussions about each lesson. Teachers must have some prerequisite knowledge of each topic before presenting it to the class in order to effectively answer any students' questions.

Assessment Plan: 0

The Faux Paw curriculum does offer a quiz for students to complete at the completion of the very last lesson. However, there is no formal plan in place for teachers to confirm that their students have comprehended the material presented.

Overall Program Score: 12

I. NETSMARTZ

Environmental Design: 1

The NetSmartz curriculum was created to help teach children ages 5–18 how to be safer on- and offline. "The program provides animations and age-appropriate interactive activities that use the latest 3-D and Web technologies to entertain the subjects while they educate" [24]. The curriculum can be used in a variety of ways: "deliver presentations to small or large assemblies, teach specific safety topics with videos and activity cards, host an Internet safety day or week, broadcast the videos through closed-circuit televisions, and can supplement acceptable use policies with Internet safety pledges" [24]. The curriculum is not fully comprehensive of computer-security concepts. Only five topics have been created for each age group. For example, the middle school topics address cyberbullying, inappropriate content, hiding personal information, meeting

offline, and future consequences of online actions. The focus of the curriculum is more centered on Internet safety rather than computer-security.

Clearly Defined Learning Objectives: 0

The purpose of the NetSmartz program is defined in the introduction and implementation guides provided in the curriculum. However, each lesson plan does not have a clear list of learning objectives.

Engaging Activities: 2

There are videos, presentations, activity worksheets, and a website that can be used along with the NetSmartz curriculum.

Classroom Displays: 2

Posters are provided in the curriculum materials. Students are afforded the opportunity to create classroom displays during specific lessons.

Reaffirmation/Reiteration of Topics: 0

The curriculum does not provide an implementation strategy that assists the teacher with incorporating the NetSmartz lessons into other subjects. Teachers are required to decide how the information should be taught along with their current approved curriculum.

Organized Time and Space: 2

Each lesson plan describes how long each activity will take and any materials needed.

Created Experiences in Response to Child's Needs: 0

Specific needs of individual children are not considered in the lesson plans.

Teachers Demonstrate Knowledge: 2

Teachers are expected to be able to facilitate classroom discussions about each lesson. Teachers must have some prerequisite knowledge of each topic before presenting it to the class in order to effectively answer any students' questions.

Assessment Plan: 0

There is no assessment plan provided by the curriculum. A teacher would be required to create their own separate testing of each student.

Overall Program Score: 9

V. SURVEY RESULTS

In our pedagogical survey of these nine cyber-security programs, there have been a number of best practices that are apparent. In the below sections we will highlight those curricula with creative approaches to teaching computer-security concepts. Table 1, on page 54, illustrates the overall scores for each program and curriculum trait.

Table 1. Curriculum Scores from Survey.

	Environmental Design	Learning Objectives	Engaging Activities	Classroom Displays	Reaffirmation of Topics	Time and Space	Special Needs	Teacher Demonstrates Knowledge	Assessment Plan	TOTALS
CERIAS	2	2	2	2	0	2	1	1	0	12
CS Unplugged	2	1	2	1	1	2	2	2	1	14
Cyber (smart:)	2	2	2	2	1	2	2	2	0	15
Cyber Smart!	2	2	2	2	2	2	2	2	0	16
CyberCitz	1	0	0	1	1	0	0	0	0	3
i-SAFE	2	2	2	2	2	1	0	2	1	14
Stay-Safe Online	1	2	1	2	0	2	0	2	0	10
iKeepSafe	1	2	2	2	2	2	0	1	0	12
NetSmartz	1	0	2	2	0	2	0	2	0	9
TOTALS	14	13	15	17	9	15	7	14	2	

A. HIGHEST-RATED PROGRAMS

The highest scoring program was Cyber Smart! with a value of 16. It had the most comprehensive program that had full examples of all the NAEYC curriculum traits except for a completed assessment plan. The next highest scoring programs with a value of 14 were: cyber(smart:) and i-SAFE. Cyber(smart:) lacked an assessment plan and a fully integrated plan of a reaffirmation of topics so that teachers could consistently refer to the concepts discussed. Along with having a very limited assessment plan, the i-SAFE program did not discuss how long a lesson would take and they were not thoughtful of individual children with learning disabilities or one's who were advanced in the topic.

B. COMMONLY MISSED CRITERIA

1. Assessment Plans

A consistently missed curriculum trait was an integration of an assessment plan into these cyber-security programs. The overall score for integrated assessment plans was a 2 out 18 possible points for all programs. If a program had created a quiz or had tried to determine the capabilities of the students after taking a lesson, then they left it up to the teacher to probe the students with questions. There was no formal plan in place to establish a baseline of ability of each student which allows a teacher to track the students' comprehension of all the cyber-security concepts.

2. Special Needs of Children

The second low scoring curriculum trait among all of the programs was the "Created Experiences in Response to Child's Needs." According to the NAEYC Accreditation All Criteria Document, "[T]eaching staff evaluate and change their responses based on individual needs. Teaching staff vary their interactions to be sensitive and responsive to: differing abilities, temperaments…cognitive and social development" [33]. The overall score for this trait was a 7 out of 18 possible points. Only three programs actually took into account children with differing cognitive abilities or previous exposure to the computer-security concepts being taught. CS Unplugged created separate activities for learners that were more advanced and gave suggestions for how teachers

should engage students with difficulty grasping the subject matter (although, not special needs education). Both cyber(smart:) and Cyber Smart! programs created sections in their lesson plans for advanced students. They were extension activities of each lesson that other students were required to execute. A benefit of having these "extra for experts" [17] sections is that teachers can "reaffirm" the completed topics during future lessons or along with their other science and technology curricula. Being responsive to child's needs and a reaffirmation of topics was evidence of a broad and fully developed computer-security program for children.

C. EFFECTIVE CURRICULUM TRAITS

After completing this pedagogical survey, we have assembled best features of the reviewed programs. Each feature is explained and then an example from a reviewed program is included. The best features are what made these programs unique among their peer programs.

1. Organization

The organization of a program defines how well it was developed, tested, and reviewed before being elected for use. This was the most important trait that we emphasized when we reviewed these curricula. A program that attempted to teach as many computer-security subjects as possible, without being repetitive, had a higher score among the other programs. A program should teach as many computer-security topics as possible and then continue to introduce new concepts to reaffirm what a student has learned previously. One very good example is the Common Sense media curriculum that focused on the following cyber-security subjects:

Figure 10. CommonSenseMedia Curriculum Category Descriptions. From [6], [7].

These eight concepts are very closely organized and the curriculum does a very good job at reaffirming these topics throughout every age group. Hypothetically, a student would learn about Internet safety if they started at age 5 and continue to learn about that subject when they completed the curriculum at age 18.

2. Ease of Use and Portability

The CS Unplugged curriculum is very unique in that they require only minimal assembly by a proctor in order to begin use. The amount of tools or materials required to use its lesson plans remain quite minimal. A teacher could use these lessons outside of the classroom in an entirely different environment. Hence, the moniker of this program is true to form. The activities employed in the information hiding example are very similar to common children's games, i.e. "telephone." An example lesson plan can be reviewed in the Appendix.

3. Multiple Learning Approaches

The cyber(smart:) program had the most creative and the largest number of learning approaches. There were a variety of resources that were created to be used as supplementary tools by educators using the curriculum. Teachers are not reliant on only one mechanism for delivering the material. A teacher can use videos, games, blogs, classroom presentations, lessons and books.

4. Narrative or Central Theme

The use of a narrative or central story of a curriculum helped to facilitate organization of each of the sub-topics. Examples of this was the Faux Paw storyline in the iKeepSafe program and the Hector's World thematic narrative used in the cyber(smart:) program. By using a story to illustrate computer security concepts, the concepts would build on past knowledge learned from a previous lesson. The chronology of the storyline helped to reaffirm concepts that were interrelated.

5. Assessment Plans

Any program can create an assessment plan for their students. It is not more or less appropriate for any specific type of program. CS Unplugged could create a written test or a set of questions that teachers could use after the completion of their lessons. The programs iKeepSafe, cyber(smart:), and CyberSmart! could all create online assessments for tracking their programs by educators. At the very least, educators should have access to a question-and-answer worksheet at the end of a sub-topic. Since many of the concepts discussed in each of these curricula are based on tangible practices, it is important that an assessment plan take this into account. An example would be that a student is required to demonstrate what is considered a secure action when they are prompted online for personal information. Another question could require a student to choose between a set of photos what would be considered appropriate to post online on a social media website. Either way a teacher plans to incorporate an assessment plan they should be very cognizant of the mission of the curriculum and be sure to reiterate the most important material.

An assessment plan can take many different forms depending on what the teacher is trying to accomplish. Assessment plans should take into account three different phases of a student's experience in a specific curriculum. These three phases include a basic exam, a quiz after each lesson or sub-topic, and then a final exam or project that determines how much a student has retained over the entire time of being exposed to the material.

a. Preliminary Assessment

A preliminary baseline of a student's knowledge could be determined by giving them a short written or oral exam over some basic cyber-security concepts. The structure of each exam should be tailored to the age group of the student. Focus should be placed on discussion of the Internet and how computers are used to access resources on the Internet. The uniqueness of the questions and difficulty should be based on the age of the students. Expectations of their cyber-security knowledge should be put in a perspective considering their possible exposure to these topics in prior grades or school programs.

b. Sub-topic Assessment

This examination of the student's capabilities should be based exclusively on the learning objectives stated at the beginning of each lesson. A teacher is then able to determine the effectiveness of the instruction addressing the goals of the curriculum for a specific topic.

c. Curriculum Completion Assessment

A final examination of each student should be given at the completion of all the concepts delivered for their specific age-group. This test should focus on key concepts and security practices that are important to each sub-topic. This assessment should be used to determine which topics need to be reiterated again or more comprehensively for that student and for future classes.

6. Utilizes Feedback

A program that is consistently restructuring and is trying to improve itself through user feedback seems to be directly connected with how well the curriculum did when reviewed by our grading criteria. Programs like cyber(smart:), Common Sense Media, Cyber Smart!, i-SAFE, and iKeepSafe all utilize some forum to gain feedback from its users. Continuous and authentic review of students' experiences assists in the advancement of the learning process. This information can further allow the curriculum to evolve and change with the needs of its audience.

VI. CONCLUSION

A. EVALUATION OF WORK

Our work has been to determine the current state of computer-security curricula available for children. We tailored our survey based on criteria guidelines of a national organization that is utilized to accredit a multitude of different educational programs. The guidelines we used may not have been entirely comprehensive of the most effective grading criteria that could have been used. However, we believe the curriculum standards that we used to complete our pedagogical survey are directly representative of highly acclaimed programs. The standards as prescribed by the NAEYC, AMLE, and NSTA are used nation-wide to determine scientific educational programs of excellence.

Our survey focused on a variety of aspects of each program. We delved into traits of each program that were concerned with the perspectives of the student and teacher, and the interaction between both parties. We were able to also determine which programs were particularly interested in evolving the product that they provide to each educator. It wasn't enough to create a curriculum and leave it to the educator to use. The very best programs strive to be easily integrated into a teacher's or administrator's current curricula. It was these programs that set the benchmark for future curriculums to model.

B. FUTURE WORK

There are a number of progressive steps our research could be applied to in the future. One study could have educators utilize the best programs from our survey in their classroom. The results from their students' experiences could be documented and compared to determine the best programs overall. This research could then be used to create a hybrid type of curriculum based on a user-centered approach that took the best traits of each program. More cyber-security concepts could be created to cover the whole spectrum of research garnered to be crucial for STEM education.

Once this hybrid curriculum has been created, further beta testing would be necessary to determine its effectiveness. Evaluation of the curriculum could be based on how much a certain set of students has learned after being exposed to the program.

Assessments should be given at the beginning, at specific intervals, and after completion. Formal analysis of the assessments could then prove how much computer-security information the children are taking away from each lesson and reveal gaps in the curriculum for improvement.

After the curriculum has been proven to be an effective learning tool, a website should be created to distribute the curriculum to anyone that wished to use it. All of the videos, lesson plans, activity worksheets, etc., should be available for download. Discussion forums should continue to be utilized and constantly monitored for feedback and new topics so that the curriculum can evolve as new subjects become a part of the computer-security landscape. Allowing the curriculum to evolve as quickly as possible to keep current with the cyber-security landscape would consistently validate its use along with all other mainstream subjects.

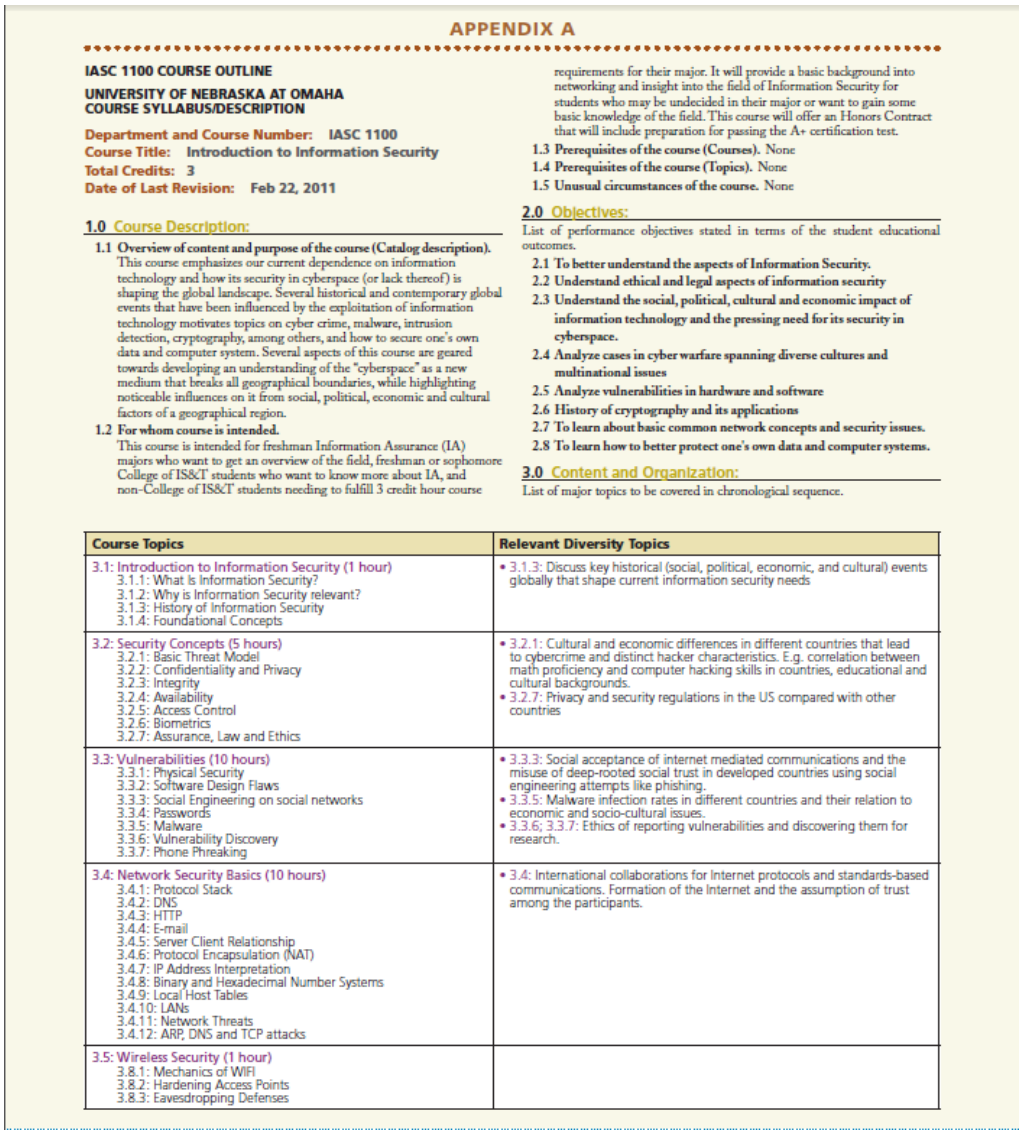
C. CONTRIBUTIONS

Our research established a plan to determine the most effective and relevant cyber-security curriculum available. We created a survey criteria based on the 3 most influential national education organizations. The results of our survey display what current cyber-security programs would be most effective for use by teachers. By completing this work, we believe that we have pointed the direction for future researchers to create and distribute a very effective and comprehensive computer-security curriculum that would benefit and educate all non-technical audiences.

APPENDIX

A. EXAMPLES OF SURVEYED CURRICULA

1. University of Nebraska-Omaha



APPENDIX A

IASC 1100 COURSE OUTLINE

UNIVERSITY OF NEBRASKA AT OMAHA
COURSE SYLLABUS/DESCRIPTION

Department and Course Number: IASC 1100
Course Title: Introduction to Information Security
Total Credits: 3
Date of Last Revision: Feb 22, 2011

1.0 Course Description:

1.1 Overview of content and purpose of the course (Catalog description). This course emphasizes our current dependence on information technology and how its security in cyberspace (or lack thereof) is shaping the global landscape. Several historical and contemporary global events that have been influenced by the exploitation of information technology motivates topics on cyber crime, malware, intrusion detection, cryptography, among others, and how to secure one's own data and computer system. Several aspects of this course are geared towards developing an understanding of the "cyberspace" as a new medium that breaks all geographical boundaries, while highlighting noticeable influences on it from social, political, economic and cultural factors of a geographical region.

1.2 For whom course is intended. This course is intended for freshman Information Assurance (IA) majors who want to get an overview of the field, freshman or sophomore College of IS&T students who want to know more about IA, and non-College of IS&T students needing to fulfill 3 credit hour course requirements for their major. It will provide a basic background into networking and insight into the field of Information Security for students who may be undecided in their major or want to gain some basic knowledge of the field. This course will offer an Honors Contract that will include preparation for passing the A+ certification test.

1.3 Prerequisites of the course (Courses). None

1.4 Prerequisites of the course (Topics). None

1.5 Unusual circumstances of the course. None

2.0 Objectives:

List of performance objectives stated in terms of the student educational outcomes.

2.1 To better understand the aspects of Information Security.
2.2 Understand ethical and legal aspects of information security
2.3 Understand the social, political, cultural and economic impact of information technology and the pressing need for its security in cyberspace.
2.4 Analyze cases in cyber warfare spanning diverse cultures and multinational issues
2.5 Analyze vulnerabilities in hardware and software
2.6 History of cryptography and its applications
2.7 To learn about basic common network concepts and security issues.
2.8 To learn how to better protect one's own data and computer systems.

3.0 Content and Organization:

List of major topics to be covered in chronological sequence.

Course Topics	Relevant Diversity Topics
3.1: Introduction to Information Security (1 hour) 3.1.1: What is Information Security? 3.1.2: Why is Information Security relevant? 3.1.3: History of Information Security 3.1.4: Foundational Concepts	• 3.1.3: Discuss key historical (social, political, economic, and cultural) events globally that shape current information security needs
3.2: Security Concepts (5 hours) 3.2.1: Basic Threat Model 3.2.2: Confidentiality and Privacy 3.2.3: Integrity 3.2.4: Availability 3.2.5: Access Control 3.2.6: Biometrics 3.2.7: Assurance, Law and Ethics	• 3.2.1: Cultural and economic differences in different countries that lead to cybercrime and distinct hacker characteristics. E.g. correlation between math proficiency and computer hacking skills in countries, educational and cultural backgrounds. • 3.2.7: Privacy and security regulations in the US compared with other countries
3.3: Vulnerabilities (10 hours) 3.3.1: Physical Security 3.3.2: Software Design Flaws 3.3.3: Social Engineering on social networks 3.3.4: Passwords 3.3.5: Malware 3.3.6: Vulnerability Discovery 3.3.7: Phone Phreaking	• 3.3.3: Social acceptance of internet mediated communications and the misuse of deep-rooted social trust in developed countries using social engineering attempts like phishing. • 3.3.5: Malware infection rates in different countries and their relation to economic and socio-cultural issues. • 3.3.6; 3.3.7: Ethics of reporting vulnerabilities and discovering them for research.
3.4: Network Security Basics (10 hours) 3.4.1: Protocol Stack 3.4.2: DNS 3.4.3: HTTP 3.4.4: E-mail 3.4.5: Server Client Relationship 3.4.6: Protocol Encapsulation (NAT) 3.4.7: IP Address Interpretation 3.4.8: Binary and Hexadecimal Number Systems 3.4.9: Local Host Tables 3.4.10: LANs 3.4.11: Network Threats 3.4.12: ARP, DNS and TCP attacks	• 3.4: International collaborations for Internet protocols and standards-based communications. Formation of the Internet and the assumption of trust among the participants.
3.5: Wireless Security (1 hour) 3.8.1: Mechanics of WIFI 3.8.2: Hardening Access Points 3.8.3: Eavesdropping Defenses	

Figure 11. IASC 1100 Course Outline. From [9].

Course Topics	Relevant Diversity Topics
3.6: Cyber War, Crime and Digital Forensics (2 hours) 3.5.1: Case study of cyber attacks and cyber wars 3.5.2: Comparing cyber warfare capabilities from different nations 3.5.3: Intrusion Detection 3.5.4: Gathering Evidence 3.5.5: Recovery	• 3.6: Discuss the social and cultural impact on governance and operations in cyberspace. • 3.5.1: Case study of cyber attacks and cyber wars in different countries. US as a target of cyber warfare. • 3.5.2: Comparing cyber warfare capabilities from different nations • 3.5.4: Balancing intelligence needs with citizen's right to privacy in US and Europe.
3.7: Ethics and Legal Controls (2 hours) 3.6.1: Government and Business Oversight 3.6.2: Hacking for Good	• 3.6.2: In-depth investigation of cyber attack cases for different social, political, cultural and economic causes. [Gandhi SPEC 2011] Reference at end of this table.
3.7: Cryptography (5 hours) 3.7.1: History and Background 3.7.2: DES, 3-DES, AES 3.7.3: PKI 3.7.4: Authentication and Integrity 3.7.5: PGP	• 3.7.1: Examination of the history of cryptography in various cultures and its impact on the course of wars. E.g. the German Enigma machine and its impact on World War II. • 3.7.2: Compare controls on the export of cryptography in US to other countries
3.8: Assurance and Risk Assessment (5 hours) 3.8.1: The need for assurance 3.8.2: Assurance throughout the lifecycle 3.8.3: Risk Components 3.8.4: Qualitative and Quantitative Risk Assessments	• 3.8: Compare assurance mechanisms in Germany, Canada, Europe, and US and their amalgamation into the Common Criteria
3.9: Policies and Procedures (5 hours) 3.9.1: CMS Model 3.9.2: Analyzing Costs and Risks 3.9.3: Disaster Plan 3.9.4: Administrative vs. Users 3.9.5: Backups 3.9.6: Security Audits	• 3.9: Consideration of social and cultural norms in defining security policies. • 3.9.2: Acceptance and enforcement of security policies in a culturally diverse workforce.

4.0 Teaching Methodology:

4.1 Methods to be used.
The course will be presented primarily in lecture form. However, students will be expected to participate in discussions of the various topics as they are studied. In addition to the study of the text, students must do homework as assigned and periodic laboratory exercises with write-ups of the exercise. Two tests will be given. A written paper with oral presentation as a semester project will be required.

4.2 Student role in the course.
The students will be involved through exams, homework, projects, laboratory exercises and discussion with each other.

4.3 Contact hours.
3 hours per week.

5.0 Evaluation:

5.1 Type of student projects that will be the basis for evaluating student performance, specifying distinction between undergraduate and graduate, if applicable. For laboratory projects, specify the number of weeks spent on each project).
Students will complete a research-oriented project in the form of a 5 – 10 page paper with a 10 minute power point presentation.

5.1.1 Research-oriented project
The objective of a research-oriented project is to study and digest advanced technical literature, and report on it in a form that is easy to understand for other students in the class. Extensiveness, comprehensibility and technical worthiness are major considerations.

5.2 Basis for determining the final grade (Course requirements and grading standards) specifying distinction between undergraduate and graduate, if applicable.
Two exams will be given during the course:
25% Exam 1
25% Exam 2
20% Semester project
10% Laboratory Assignments
10% Homework Assignments
10% Daily Written Assignments
Tentatively, exams are scheduled every seven weeks.

Daily Written Assignments
Students are expected to bring to class each day, except on test days, a written paragraph summary, in your own words, of a current event article dealing with information security. There are many online sources for daily information security news such as: slashdot.org and www.securityfocus.com. These are only a couple of many possible sites and students should find others on your own by doing a search.

These assignments will be discussed each day so students need to be prepared to present their assignment. Additionally, students must include one question with answer that would make a good test question, based upon the previous class period's lecture or activity.

5.3 Grading scale and criteria.

A+	97% - 100%	
A	93% - 96%	
A-	90% - 92%	
B+	87% - 89%	
B	83% - 86%	
B-	80% - 82%	
C+	77% - 79%	
C	73% - 76%	Minimum final, passing grade for Engineering
C-	70% - 72%	Minimum final, passing grade for IS&T students
D+	67% - 69%	
D	63% - 66%	
D-	60% - 62%	
F	00% - 59%	

6.0 Resource Material

6.1 Textbooks and/or other required readings used in course.
Rick Lehtinen, Deborah Russell, and G.T. Gangemi Sr., *Computer Security Basics (Second Edition)*, O'Reilly, 2006.

6.2 Other suggested reading materials, if any.
6.2.1 Ross Anderson, *Security Engineering*, Wiley, 2001.
6.2.2 Bruce Schneier, *Beyond Fear*, Copernicus Books, 2003.

6.3 Other sources of information.
Research publications may be distributed and studied to better understand the topics in question.

Figure 12. IASC 1100 Course Outline, page 2. From [9].

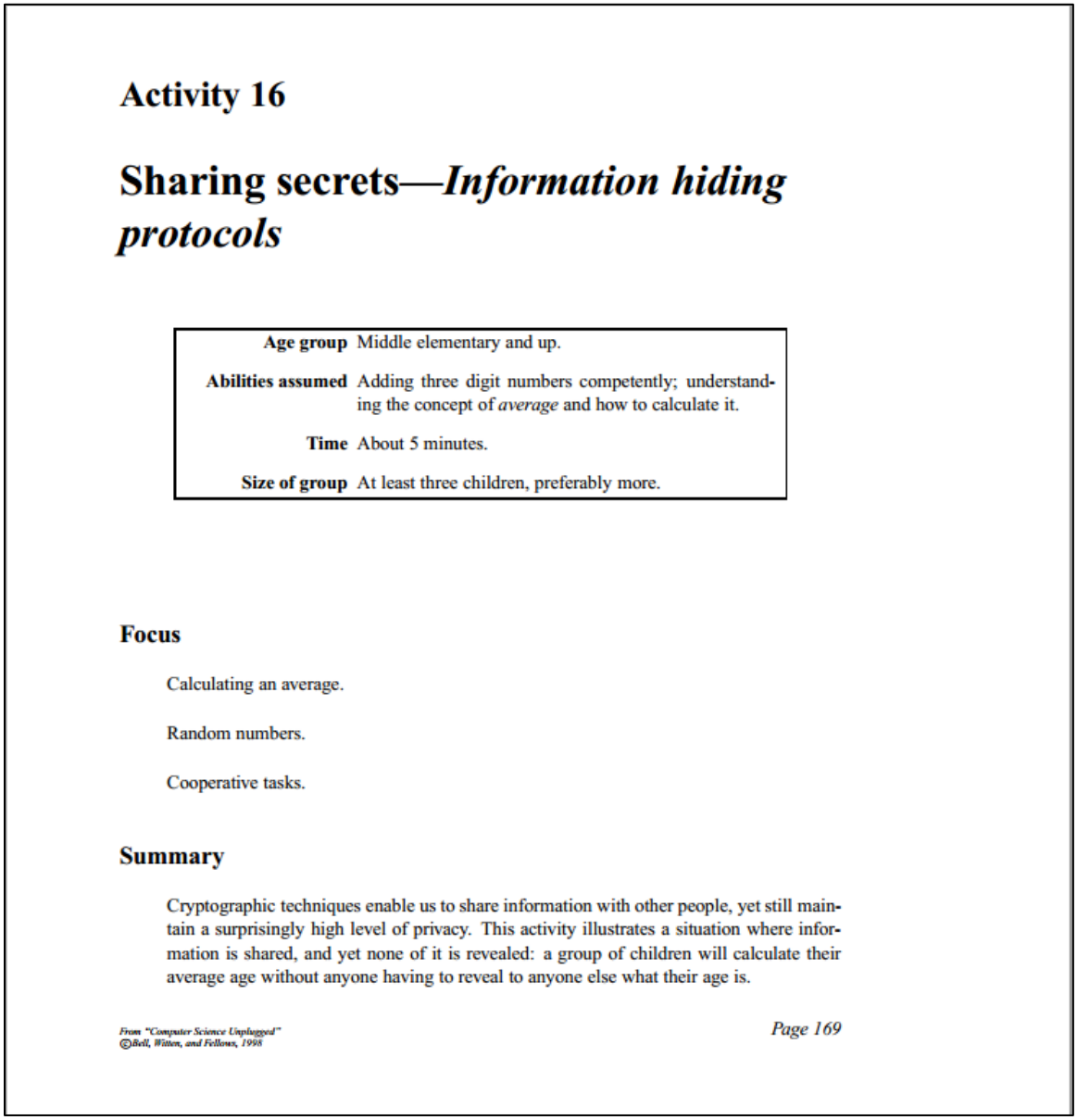
2. U.S. Naval Academy

/SI110/Outline

SI110		Introduction
	The Cyber Battlefield	Digital Data 1 & 2
		The Physical Computer
		PC Vivisection
		Operating Systems 1 & 2, Operating Systems 3
		Programs Part 1 & Part 2 & 3, Part 4, Part 5
		Web: Servers, browsers and HTML
		Web: Build your webpage
		Web: Client Side Scripting: non-event driven, event driven, forms
		Web: Server Side Scripting
		Web: Injection attacks & XSS
		Networks, Protocols, the Internet: Part 1, Part 2, Part 3 & 4
		Networks: build-a-lan prep
		Networks: build-a-lan lab
		Networks: wireless networking
		Networks: build-a-wireless-network lab
	Models and Tools	Information Assurance
		Firewalls
		Symmetric Encryption
		Hashing
		Digital Cryptography
		Asymmetric Cryptography
		Authentication/Crypto: X.509 certificates lab
		Steganography
	Cyber Operations	Forensics
		Forensics Lab
		Phases of a cyber attack / recon
		Network Attack
		Network Defense
		Malware
		Case Studies
		Cyber Recon Lab
		Cyber Attack Lab
		Cyber Defense Lab

Figure 13. SI110 Course Outline for CyberSecurity Course, Mandatory for all Midshipmen. From [37].

3. CS Unplugged



Activity 16

Sharing secrets—*Information hiding protocols*

Age group	Middle elementary and up.
Abilities assumed	Adding three digit numbers competently; understanding the concept of *average* and how to calculate it.
Time	About 5 minutes.
Size of group	At least three children, preferably more.

Focus

Calculating an average.

Random numbers.

Cooperative tasks.

Summary

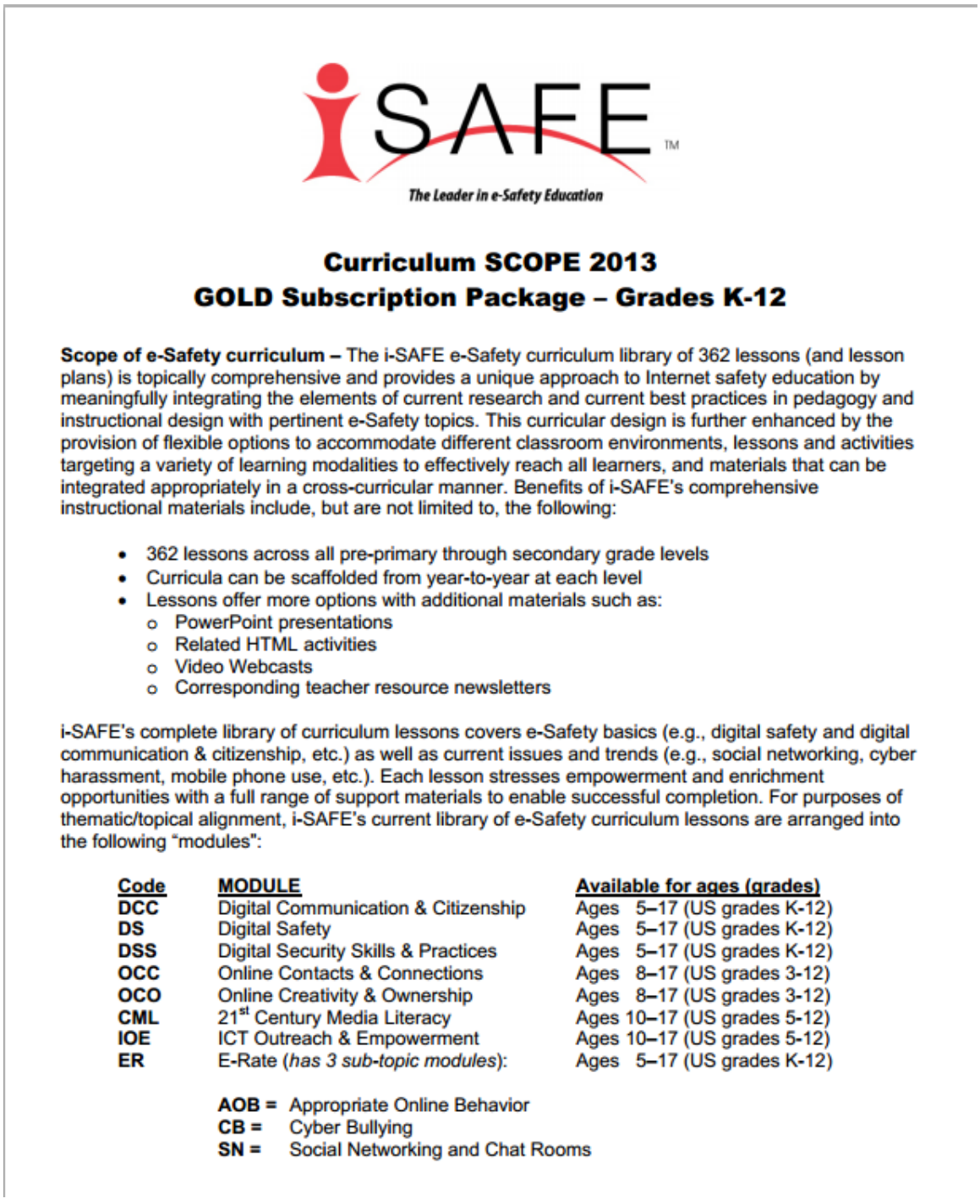
Cryptographic techniques enable us to share information with other people, yet still maintain a surprisingly high level of privacy. This activity illustrates a situation where information is shared, and yet none of it is revealed: a group of children will calculate their average age without anyone having to reveal to anyone else what their age is.

From "Computer Science Unplugged"
©Bell, Witten, and Fellows, 1998

Page 169

Figure 14. CS Unplugged Lesson Plan for Information Hiding. From [15].

4. i-SAFE Curriculum



Curriculum SCOPE 2013
GOLD Subscription Package – Grades K-12

Scope of e-Safety curriculum – The i-SAFE e-Safety curriculum library of 362 lessons (and lesson plans) is topically comprehensive and provides a unique approach to Internet safety education by meaningfully integrating the elements of current research and current best practices in pedagogy and instructional design with pertinent e-Safety topics. This curricular design is further enhanced by the provision of flexible options to accommodate different classroom environments, lessons and activities targeting a variety of learning modalities to effectively reach all learners, and materials that can be integrated appropriately in a cross-curricular manner. Benefits of i-SAFE's comprehensive instructional materials include, but are not limited to, the following:

- 362 lessons across all pre-primary through secondary grade levels
- Curricula can be scaffolded from year-to-year at each level
- Lessons offer more options with additional materials such as:
  - PowerPoint presentations
  - Related HTML activities
  - Video Webcasts
  - Corresponding teacher resource newsletters

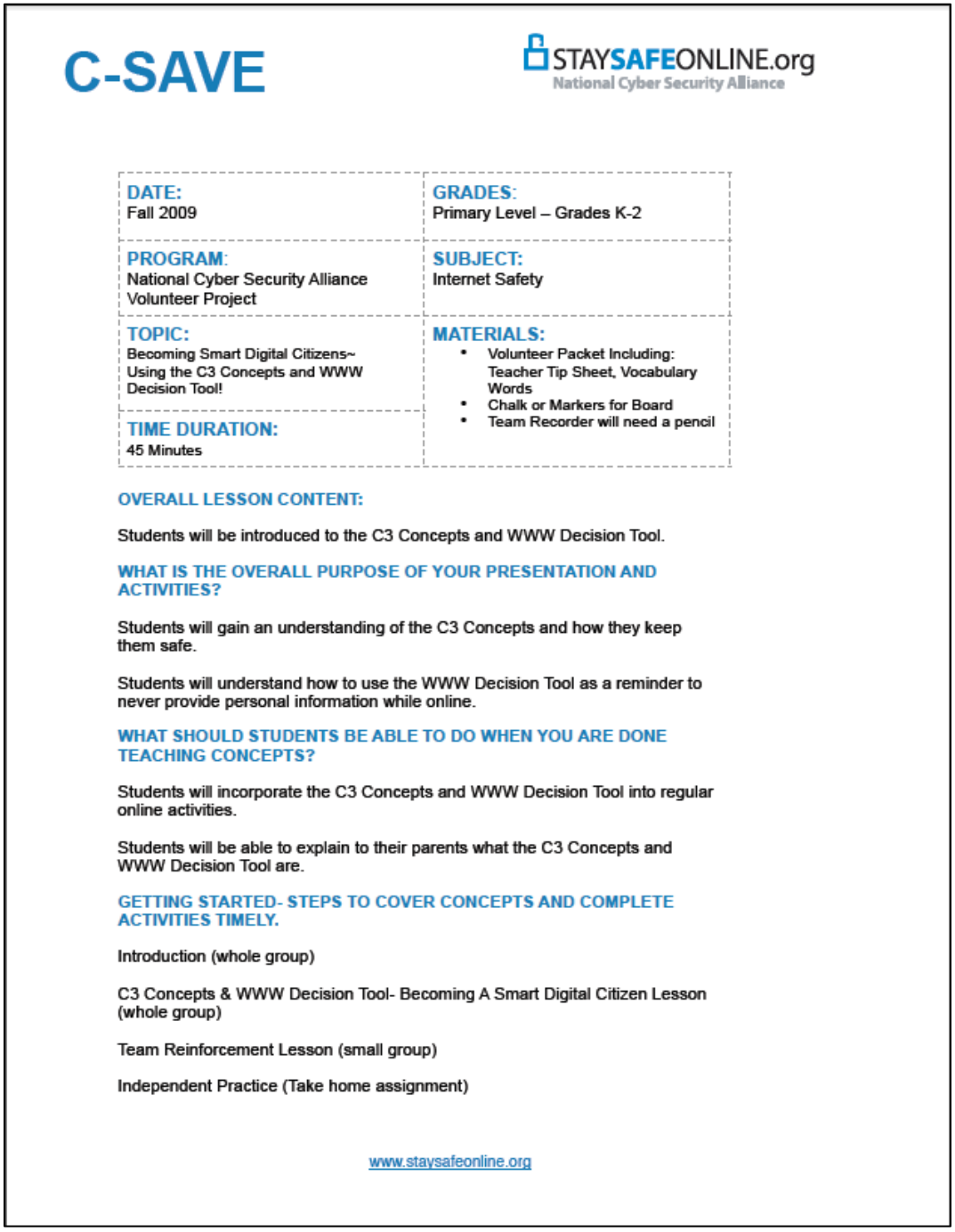
i-SAFE's complete library of curriculum lessons covers e-Safety basics (e.g., digital safety and digital communication & citizenship, etc.) as well as current issues and trends (e.g., social networking, cyber harassment, mobile phone use, etc.). Each lesson stresses empowerment and enrichment opportunities with a full range of support materials to enable successful completion. For purposes of thematic/topical alignment, i-SAFE's current library of e-Safety curriculum lessons are arranged into the following "modules":

Code	MODULE	Available for ages (grades)
DCC	Digital Communication & Citizenship	Ages 5–17 (US grades K-12)
DS	Digital Safety	Ages 5–17 (US grades K-12)
DSS	Digital Security Skills & Practices	Ages 5–17 (US grades K-12)
OCC	Online Contacts & Connections	Ages 8–17 (US grades 3-12)
OCO	Online Creativity & Ownership	Ages 8–17 (US grades 3-12)
CML	21st Century Media Literacy	Ages 10–17 (US grades 5-12)
IOE	ICT Outreach & Empowerment	Ages 10–17 (US grades 5-12)
ER	E-Rate (*has 3 sub-topic modules*):	Ages 5–17 (US grades K-12)

AOB = Appropriate Online Behavior
CB = Cyber Bullying
SN = Social Networking and Chat Rooms

Figure 15. I-SAFE Curriculum Scope Description. From [19].

5. StaySafeOnline



C-SAVE

STAYSAFEONLINE.org
National Cyber Security Alliance

DATE: Fall 2009	**GRADES:** Primary Level – Grades K-2
PROGRAM: National Cyber Security Alliance Volunteer Project	**SUBJECT:** Internet Safety
TOPIC: Becoming Smart Digital Citizens~ Using the C3 Concepts and WWW Decision Tool!	**MATERIALS:** • Volunteer Packet Including: Teacher Tip Sheet, Vocabulary Words • Chalk or Markers for Board • Team Recorder will need a pencil
TIME DURATION: 45 Minutes	

OVERALL LESSON CONTENT:

Students will be introduced to the C3 Concepts and WWW Decision Tool.

WHAT IS THE OVERALL PURPOSE OF YOUR PRESENTATION AND ACTIVITIES?

Students will gain an understanding of the C3 Concepts and how they keep them safe.

Students will understand how to use the WWW Decision Tool as a reminder to never provide personal information while online.

WHAT SHOULD STUDENTS BE ABLE TO DO WHEN YOU ARE DONE TEACHING CONCEPTS?

Students will incorporate the C3 Concepts and WWW Decision Tool into regular online activities.

Students will be able to explain to their parents what the C3 Concepts and WWW Decision Tool are.

GETTING STARTED- STEPS TO COVER CONCEPTS AND COMPLETE ACTIVITIES TIMELY.

Introduction (whole group)

C3 Concepts & WWW Decision Tool- Becoming A Smart Digital Citizen Lesson (whole group)

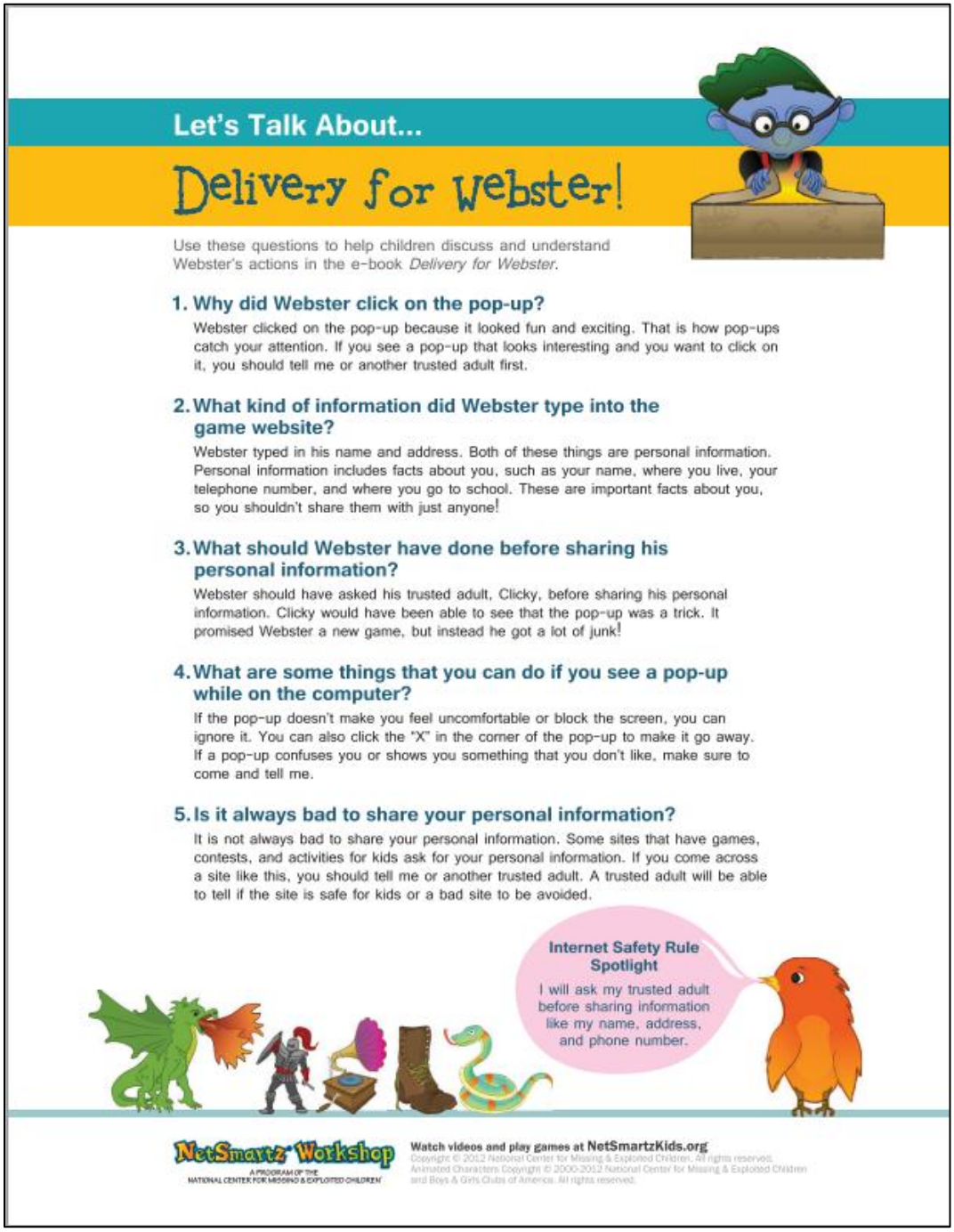
Team Reinforcement Lesson (small group)

Independent Practice (Take home assignment)

www.staysafeonline.org

Figure 16. StaySafeOnline Activity Sheet Example. From [36].

6. NetSmartz



Let's Talk About...

Delivery for Webster!

Use these questions to help children discuss and understand Webster's actions in the e-book *Delivery for Webster*.

1. Why did Webster click on the pop-up?

Webster clicked on the pop-up because it looked fun and exciting. That is how pop-ups catch your attention. If you see a pop-up that looks interesting and you want to click on it, you should tell me or another trusted adult first.

2. What kind of information did Webster type into the game website?

Webster typed in his name and address. Both of these things are personal information. Personal information includes facts about you, such as your name, where you live, your telephone number, and where you go to school. These are important facts about you, so you shouldn't share them with just anyone!

3. What should Webster have done before sharing his personal information?

Webster should have asked his trusted adult, Clicky, before sharing his personal information. Clicky would have been able to see that the pop-up was a trick. It promised Webster a new game, but instead he got a lot of junk!

4. What are some things that you can do if you see a pop-up while on the computer?

If the pop-up doesn't make you feel uncomfortable or block the screen, you can ignore it. You can also click the "X" in the corner of the pop-up to make it go away. If a pop-up confuses you or shows you something that you don't like, make sure to come and tell me.

5. Is it always bad to share your personal information?

It is not always bad to share your personal information. Some sites that have games, contests, and activities for kids ask for your personal information. If you come across a site like this, you should tell me or another trusted adult. A trusted adult will be able to tell if the site is safe for kids or a bad site to be avoided.

Internet Safety Rule Spotlight

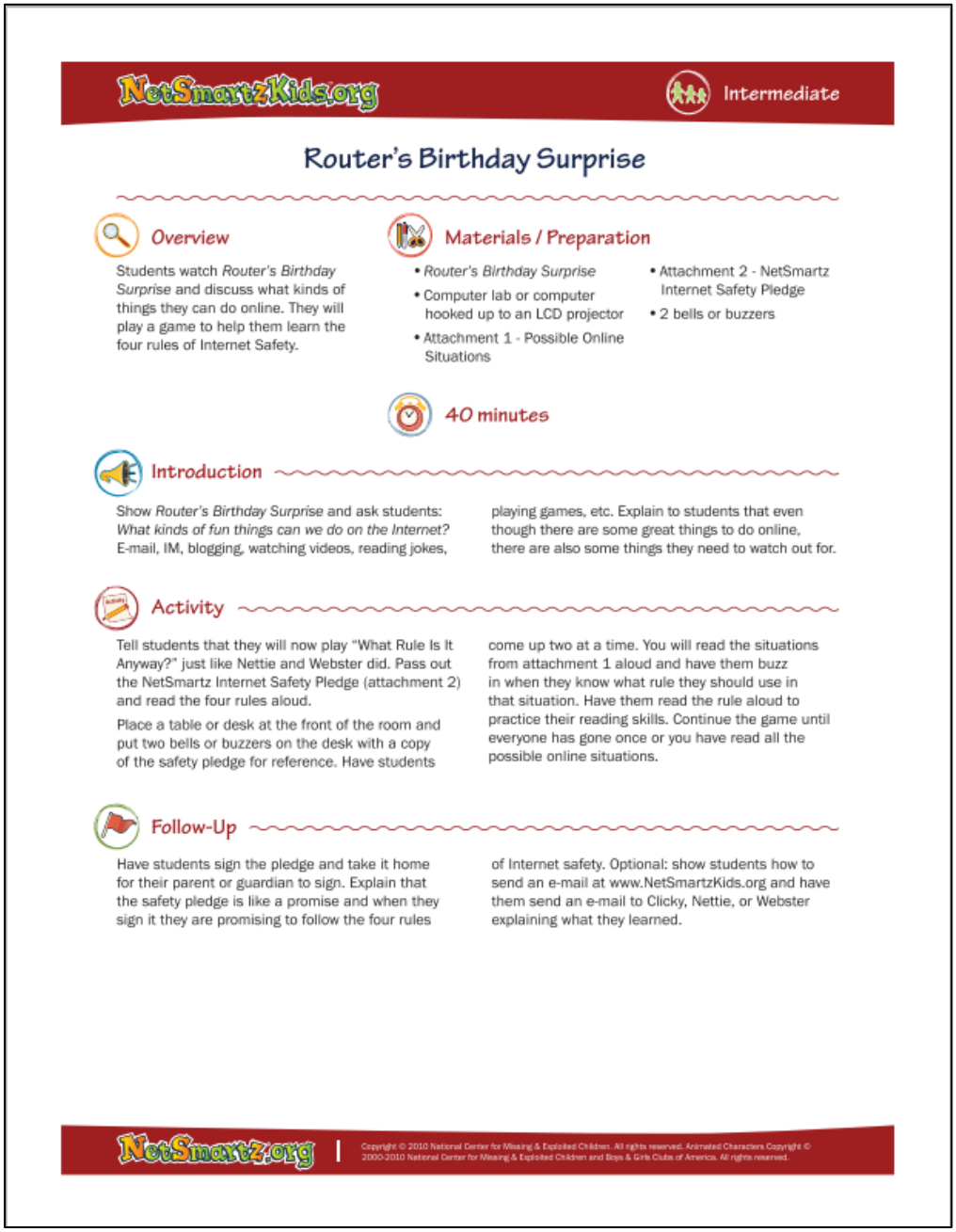
I will ask my trusted adult before sharing information like my name, address, and phone number.

NetSmartz Workshop
A PROGRAM OF THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Watch videos and play games at NetSmartzKids.org

Figure 17. NetSmartz Discussion Handout—Information Hiding. From [24].

7. NetSmartz



NetSmartzKids.org

Intermediate

Router's Birthday Surprise

Overview

Students watch *Router's Birthday Surprise* and discuss what kinds of things they can do online. They will play a game to help them learn the four rules of Internet Safety.

Materials / Preparation

- *Router's Birthday Surprise*
- Computer lab or computer hooked up to an LCD projector
- Attachment 1 - Possible Online Situations
- Attachment 2 - NetSmartz Internet Safety Pledge
- 2 bells or buzzers

40 minutes

Introduction

Show *Router's Birthday Surprise* and ask students: *What kinds of fun things can we do on the Internet?* E-mail, IM, blogging, watching videos, reading jokes, playing games, etc. Explain to students that even though there are some great things to do online, there are also some things they need to watch out for.

Activity

Tell students that they will now play "What Rule Is It Anyway?" just like Nettie and Webster did. Pass out the NetSmartz Internet Safety Pledge (attachment 2) and read the four rules aloud.

Place a table or desk at the front of the room and put two bells or buzzers on the desk with a copy of the safety pledge for reference. Have students come up two at a time. You will read the situations from attachment 1 aloud and have them buzz in when they know what rule they should use in that situation. Have them read the rule aloud to practice their reading skills. Continue the game until everyone has gone once or you have read all the possible online situations.

Follow-Up

Have students sign the pledge and take it home for their parent or guardian to sign. Explain that the safety pledge is like a promise and when they sign it they are promising to follow the four rules of Internet safety. Optional: show students how to send an e-mail at www.NetSmartzKids.org and have them send an e-mail to Clicky, Nettie, or Webster explaining what they learned.

NetSmartz.org |

Figure 18. NetSmartz Example Activity Worksheet—Internet Safety. From [24].

LIST OF REFERENCES

[1] Symantec Corporation. (2013, April). Security response publications–annual threat report [Online]. Available: http://www.symantec.com/security_response/publications/

[2] M. Swanson and B. Guttman, "Generally accepted principles and practices for securing information technology systems," National Institute of Standards and Technologies, Gaithersburg, MD, Publication 800–14, September 1996.

[3] National Institute of Standards and Technology. (2010, November 05). National cybersecurity workforce framework, [Online]. Available: http://csrc.nist.gov/nice/framework/

[4] Common Sense Media. (2013, January). K-2 digital literacy & citizenship curriculum. [Online]. Available: http://www.commonsensemedia.org/educators/curriculum/grades-k-2.

[5] Common Sense Media. (2012). Our k-12 digital literacy and citizenship curriculum. [Online]. Available: http://www.commonsensemedia.org/sites/default/files/curriculum-overview.pdf

[6] U.S. Department of Commerce, Census Bureau, (2011) "Digest of education statistics – 2011 annual report," U.S. Department of Commerce, Washington, D.C., Rep. NCES 2012–001, May 2012.

[7] R. Ghandi, C. Jones and W. Mahoney, "A freshman level course on information assurance: Can it be done? Here's how," *ACM Inroads*, vol. 3, no. 3, pp. 50–61, 2012.

[8] C. Brown et al., "Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States Naval Academy," in *ITiCSE*, 2012, pp.303–308.

[9] Committee on National Security Systems, United States Government, (2013) *Policies*. [Online]. Available: https://www.cnss.gov/policies.html

[10] J. Schumacher, "Educating leaders in information assurance," *IEEE Transactions on Education*, vol. 45, no. 2, pp. 194–201, 2002.

[11] D. Welch and J. Schumacher, "Educating leaders in information assurance," *IEEE Transacations on Education*, vol. 45, no. 2, pp. 194–202, May 2002.

[12] Purdue University CERIAS, (2013). The k-5 information security curriculum. [Online]. Available: http://www.cerias.purdue.edu/site/education/k-12/infosec_activities/k5#contentstart

[13] T. Bell, I. H. Witten and M. Fellows, (2008, May 08). Computer science unplugged – information hiding lesson plan. [Online]. Available: http://csunplugged.org/sites/default/files/activity_pdfs_full/unplugged-16-information_hiding_0.pdf

[14] National Council of Women and Information Technology, "NCWIT progress report from Washington, D.C." Boulder, CO, September 2010.

[15] Australian Communications and Media Authority - ACMA, (2008, May). cyber(smart:). [Online]. Available: http://www.cybersmart.gov.au/young%20kids.aspx

[16] S. C. Knickrem et al., (2007, December). Cyber citizenship educators' guide. [Online]. Available: http://www.jmu.edu/iiia/wm_preview/citizenguide.shtml

[17] i-SAFE, (2002) i-SAFE, the leader in e-safety education solutions. [Online]. Available: http://isafe.org/wp/?page_id=211

[18] U.S. Department of Homeland Security, (2010, October 10). Stop.think.connect. cyber awareness coalition. [Online]. Available: http://www.dhs.gov/stopthinkconnect

[19] National Cybersecurity Alliance, (2013). Stay safe online – grades k-2. [Online]. Available: http://www.staysafeonline.org/teach-online-safety/grades-k-2

[20] iKeepSafe, (2013). iKeepSafe mission & vision. [Online]. Available: http://www.ikeepsafe.org/about-us/mission-vision/

[21] iKeepSafe, (2013) Welcome, Educators!. [Online]. Available: http://www.ikeepsafe.org/educators/

[22] National Center for Missing and Exploited Children, (2001) Netsmartz. [Online]. Available: http://origin.www.netsmartz.org/Overview/AboutUs

[23] Multi-State Information Sharing & Analysis Center, (2013). Mission & objectives. [Online]. Available: http://msisac.cisecurity.org/about/

[24] Ohio Homeland Security Advisory Council, (2011, October). State of Ohio cyber-security strategy. [Online]. Available: http://infragard.columbus.oh.us/docs/Ohio_Cyber_Strategy_11022011.doc

[25] P. Balaraman et al., (1995, October).Strategies for effective teaching, a handbook for teaching assistants. [Online]. Available: http://www.engr.wisc.edu/services/elc/strategies.pdf

[26] D. C. Orlich et al., *Teaching Strategies: A Guide to Effective Instruction*, Boston, MA: Wadsworth Cengage Learning, 2013.

[27] S. Cooper et al., “An Exploration of the Current State of Information Assurance Education,” ACM SIGCSE Bulletin, vol. 41, pp 109–125, December 2009.

[28] National Association for the Education of Young Children, (2013). Overview of naeyc. [Online]. Available: http://www.naeyc.org/content/about-naeyc

[29] Association for Middle Level Education, (2010, August). Essential attributes and characteristics of successful schools. [Online]. Available: http://www.amle.org/AboutAMLE/ThisWeBelieve/The16Characteristics/tabid/1274/Default.aspx

[30] National Science Teachers Association, (1998, January). The national science education standards. [Online]. Available: http://www.nsta.org/about/positions/standards.aspx

[31] National Association for the Education of Young Children, (2013, April 01). Accreditation criteria document. [Online]. Available: http://www.naeyc.org/files/academy/file/AllCriteriaDocument.pdf

[32] International Society for Technology in Education, (2011). Computational thinking vocabulary and progression chart. [Online]. Available: http://www.iste.org/learn/computational-thinking/ct-toolkit

[33] International Society for Technology in Education, (2011). Computational thinking leadership toolkit. [Online]. Available: http://www.iste.org/docs/ct-documents/ct-leadershipt-toolkit.pdf?sfvrsn=4

[34] National Cybersecurity Alliance, (2009, September). StaySafeOnline.org teach online safety – middle & high school. [Online]. Available: http://www.staysafeonline.org/teach-online-safety/middle-and-high-school/

[35] Computer Science Department of U.S. Naval Academy, (2013, January). SI110 course outline. [Online]. Available: http://www.usna.edu/CS/si110/lec/index.html

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California